UNODC
United Nations Office on Drugs and Crime

UNITED NATIONS SECURITY COUNCIL
COUNTER-TERRORISM COMMITTEE
EXECUTIVE DIRECTORATE (CTED)

DATA DISCLOSURE FRAMEWORK (DDF)

GENERAL PRACTICES DEVELOPED BY INTERNATIONAL SERVICE PROVIDERS IN RESPONDING TO OVERSEAS GOVERNMENT REQUESTS FOR DATA

UNITED NATIONS OFFICE ON DRUGS AND CRIME

UNITED NATIONS SECURITY COUNCIL COUNTER-TERRORISM COMMITTEE EXECUTIVE DIRECTORATE

DATA DISCLOSURE FRAMEWORK

General practices developed by international service providers in responding to overseas government requests for data

In collaboration with:

United Nations
Vienna, 2021

DISCLAIMER: This document is not meant to be legal advice, and it is to be clarified that companies should always first consult their lawyers/national business associations on whether they are legally allowed to respond to any overseas requests in their jurisdiction.

Important note

All information in this document was cross-checked at the time of publication, and some parts may become outdated if there are changes and developments after the publication. It is incumbent on practitioners to ensure they are following the most up-to-date procedures and laws by consulting with competent local authorities or business associations. This publication can be downloaded at the UNODC Electronic Evidence Hub

© United Nations, August 2021. All rights reserved.

The designations employed and the presentation of material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries.

Information on uniform resource locators and links to Internet sites contained in the present publication are provided for the convenience of the reader and are correct at the time of issue. The United Nations takes no responsibility for the continued accuracy of that information or for the content of any external website.

This publication has not been formally edited.

Publishing production: English, Publishing and Library Section, United Nations Office at Vienna.

Introduction 1
The rights of users 2
Preservation 3
Cross-border voluntary disclosure 4
Mutual Legal Assistance 5
Trends and challenges 6
Annexes I II III IV V
Abbreviations
Glossary

FOREWORD

Digital is the new normal. The Internet is now a natural extension of our daily lives with over 4 billion users worldwide. Digital tools and the Internet, while mostly used to enhance our lives, are also employed by some for illicit purposes. To address the growth of crimes involving electronic evidence, particularly those facilitated by and committed on the Internet, we must stay one step ahead, by strengthening our knowledge and skills while improving inter-agency and international cooperation.

Security Council resolutions 2322 (2016) and 2396 (2017) recognized the importance of re-evaluating methods and best practices, particularly those related to electronic evidence, as well as the challenges faced by Member States in obtaining admissible electronic evidence, stressing the importance of the capacity of Member States to cooperate with the private sector in accordance with applicable law.

To assist in the implementation of these resolutions, this Data Disclosure Framework was developed to improve communication and cooperation between the public and private sectors in their handling of electronic evidence, in line with international human rights laws and the principles of necessity and proportionality.

The present framework is the result of active collaboration among the United Nations Office on Drugs and Crime (UNODC), the Counter-Terrorism Committee Executive Directorate (CTED), Member States, private sector Internet/communications service providers, academia and international organizations.

In order to prevent the exploitation of new technologies by terrorist and other organized criminal groups, all stakeholders, both public and private, need to work together. We are hopeful that this Data Disclosure Framework will provide in-depth learning and knowledge-sharing opportunities to achieve this goal.

Masood Karimipour, Chief of Terrorism Prevention Branch, United Nations Office on Drugs and Crime

Michèle Coninsx, Executive Director, Counter-Terrorism Committee Executive Directorate

Dan Svantesson, Professor, Faculty of Law, Bond University

Vivek Narayanadas, Vice President, Legal & Data Protection Officer, Shopify

CONTENTS

Foreword iii
Acknowledgements vi
Abbreviations viii
Executive summary ix

CHAPTER 1. INTRODUCTION 1

1.1 Purpose of the Data Disclosure Framework 2
1.2 Context 2
1.3 General practices 4
1.3.1 Roles and responsibilities 4
1.3.2 Scope of e-evidence 4
1.3.3 Law enforcement guidelines offered by service providers 7
1.4 Useful resources 8

CHAPTER 2. THE RIGHTS OF USERS 9

2.1 Human rights and data processing . . . 10
2.1.1 United Nations and international legal standards 10
2.1.2 Useful resources on human rights 12
2.1.3 Preservation, data retention and data protection 13
2.1.4 General Data Protection Regulation 14
2.1.5 Other examples of data protection and privacy legislations 16
2.2 User control over their data 17
2.2.1 User consent 17
2.2.2 User download 18
2.3 User notification 18

CHAPTER 3. PRESERVATION 21

3.1 Basic concepts 22
3.2 Preservation essentials 23
3.2.1 Providing useful information before receiving requests 23
3.2.2 Receiving a preservation request from an overseas State authority 24
3.2.3 Format of the preservation request 24
3.2.4 Extending 25
3.2.5 Model scenario 26
3.3 Preservation request checklist 29

CHAPTER 4. CROSS-BORDER VOLUNTARY DISCLOSURE 31

4.1 Basic concepts 32
4.2 Human rights safeguards 33
4.3 Non-emergency voluntary disclosure . . 33
4.3.1 Receiving requests 33
4.3.2 Model scenario 35
4.4.3 Non-emergency voluntary disclosure checklist 38
4.4 Emergency voluntary disclosure 41
4.4.1 Emergency v. urgency 42
4.4.2 Information to be provided in an emergency request 42
4.4.3 Model scenario 43
4.4.4 Voluntary disclosure checklists for emergency and non-emergency 46

CHAPTER 5. MUTUAL LEGAL ASSISTANCE 49

5.1 Basic concepts 50
5.2 General practices 52
5.2.1 Requesting data 52
5.2.2 Data production 52
5.2.3 Non-disclosure and sealing 53

CHAPTER 6. TRENDS AND CHALLENGES 55

6.1 Quasi-judicial role of SPs 56
6.2 Jurisdiction and the Cloud 56
6.2.1 Legal challenges 56
6.2.2 Law reform 57
6.3 Transborder data flows 59
6.4 Hosting or multilayered providers 59

ANNEXES 61

I. Sample law enforcement guidelines 62
II. Model preservation request form 64
III. Model emergency disclosure request form 69
IV. Model direct request form for voluntary disclosure 74
V. Data retention laws for selected States 79

Glossary 81

ACKNOWLEDGEMENTS

UNODC and CTED wish to thank the Governments of France, Germany, Japan, the United Kingdom of Great Britain and Northern Ireland, and the United States of America for funding the development and dissemination of the Data Disclosure Framework, as well as for the organization of an outreach workshop in the San Francisco Bay Area of the United States in July 2018, a joint meeting of the Global Initiative and Internet and Jurisdiction Policy Network in New York City in November 2019, and a virtual expert group meeting in October 2020. A series of bilateral meetings with service providers also took place after the outreach workshop in San Francisco.[1]

Special thanks go to the SIRIUS team[2] for their collaborative team work on the production of the amended Model Request Forms, and Eurojust for their contribution for annex I. We also thank the Internet and Jurisdiction Policy Network for their collaboration in the joint meeting in November 2019.

We thank the service providers, independent experts and academics who contributed invaluable input to this document (in alphabetical order of their entity):

- Lim, May-Ann, Executive Director, Asia Cloud Computing Organization
- Klaus Landefeld, Vice-Chairman of the Management Board, Director Infrastructure and Network, Association of the Internet Industry (eco.de)
- Dan Svantesson, Professor, Bond University
- Furqan Siddiqui, Careem
- Kamran Khan, Head of Safety and Security, Careem
- Sean Li, Legal Counsel and Head of Policy, Trust and Safety, Discord (until December 2020)
- Shane Glynn, Legal Counsel and Head of Policy, Trust and Safety, Discord (from January 2021)
- Alicja Smardz, Asset Protection Investigator, Ebay
- Mark Shippam, EMEA/APAC Manager Asset Protection, Ebay
- Maximilian Schubert, President, European Internet Services Providers' Association (EuroISPA) (until November 2020)
- Nima Binara, Counsel, Google
- Pat Burke, Independent consultant
- Andreas Gruber, Legal adviser, Internet Service Providers Austria (ISPA)
- Mariusz Zurawek, Founder, JustPaste.It
- Rolando Vega, Head of Law Enforcement and Government Operations, Pinterest
- Elizabeth Bacon, Senior Director, Policy and Privacy, Public Interest Registry (PIR)
- Vivek Narayanadas, Vice-President, Legal and Data Protection Officer, Shopify
- Graeme Bunton, Head of Policy, Tucows
- Reg Levy, Head of Compliance, Tucows
- Jacob Rogers, Legal Counsel, Wikimedia

[1] Compiled list of participants in all meetings:
Member States: Brazil (Federal Prosecutor's Office), Canada (Department of Global Affairs and Department of Justice), Ireland (Department of Justice and Equality), United States (Department of Justice, Secret Service). *Service providers*: After School, Asia Cloud Computing Organization, Apple, Association of the Internet Industry (eco.de), Averon, Bluehost, Careem, Discord, EuroISPA, Ebay, Facebook, Google, ISPA, JustPaste.It, MediaFire, Microsoft, Pinterest, Public Interest Registry (PIR), Shopify, Soundcloud, Telefonica, Tiktok, Tucows, Uber, Verisign, Wickr, Wikimedia. *International/multi-stakeholder organizations*: European Union (Council of the European Union, Eurojust, European Commission – DG HOME, Europol) EuroMed Police, Tech Against Terrorism. *Academia, law firms and civil society*: New America Foundation, Center for Democracy & Technology (CDT), Electronic Frontier Foundation (EFF), Georgia Institute of Technology, Internet & Jurisdiction Policy Network, Jamil & Jamil, Mayer Brown LLP.

[2] The SIRIUS Project Phase II is implemented by Europol and Eurojust.

The collaborative relationship developed within the framework of this project represents good practices to be emulated in the context of future efforts to promote international law enforcement and judicial cooperation in countering terrorism and transnational organized crime.

The Data Disclosure Framework (DDF) was conceptualized and elaborated by the UNODC Lead Expert and consultant Daniel Suter, and was further developed and finalized by Hansol Park, UNODC staff member, in close consultation with DDF Expert Group members. Citlalin Castañeda, UNODC staff member, highlighted the need for compliance with international human rights laws. The document takes into full account the developments and negotiations at regional and international level.

The Global Initiative on Handling Electronic Evidence Across Borders and the development of the present document was coordinated and led by Arianna Lepore, UNODC staff member, and Marc Porret, CTED staff member.

ABBREVIATIONS

BSI	Basic subscriber information
CTED	Counter-Terrorism Committee Executive Directorate, Security Council
ECPA	Electronic Communications Privacy Act
EDR	Emergency disclosure request
GDPR	General Data Protection Regulation
HRC	United Nations Human Rights Committee, the body that monitors implementation of the International Covenant on Civil and Political Rights
IAP	International Association of Prosecutors
ICCPR	International Covenant on Civil and Political Rights
MLA	Mutual legal assistance
OIA	Office of International Affairs - Central authority for the United States
OHCHR	United Nations Office of the High Commissioner for Human Rights
SP	Service provider

EXECUTIVE SUMMARY

The Security Council in its resolution 2396 (2017) noted with concern, "that terrorists craft distorted narratives, which are utilized to polarize communities, recruit supporters and foreign terrorist fighters, mobilize resources and garner support from sympathizers, in particular by exploiting information and communications technologies, including through the Internet and social media".

As terrorists and organized criminals increasingly use the Internet, social media and encrypted messaging apps to advance their criminality, securing evidence from providers of these services is vital. Electronic evidence stored by service providers can prove where a crime was committed, disclose incriminating communications and determine the location of offenders. Obtaining this electronic evidence can ensure those who perpetrate serious offences are brought to justice. Increasingly, overseas law enforcement and judicial authorities are using lawful mechanisms to directly contact Internet/communications service providers to preserve and request voluntary disclosure of data.

In four resolutions, 2322 (2016), 2331 (2016), 2341 (2017) and 2396 (2017), the Security Council called upon Member States that evidence shall be collected and preserved so that investigations and prosecutions may occur to hold accountable those responsible for terrorist attacks. Resolution 2322 (2016) specifically noted the significant increase in the requests for cooperation in gathering evidence from the Internet and stressed the importance of considering the re-evaluation of methods and best practices, as appropriate, in particular, related to investigative techniques and electronic evidence.

To respond to this challenge, the Counter-Terrorism Committee Executive Directorate (CTED), the United Nations Office on Drugs and Crime (UNODC) and the International Association of Prosecutors (IAP) launched a Global Initiative to strengthen the capacity of law enforcement and criminal justice officials in preserving and obtaining necessary and proportionate data in counter-terrorism cross-border investigations. An essential component of this Initiative was to engage with the service providers to enable overseas authorities to understand their procedures for preservation and voluntary disclosure requests. Several meetings were organized in this regard: an outreach workshop in the San Francisco Bay Area of the United States in July 2018, a joint meeting of the Global Initiative and the Internet & Jurisdiction Policy Network in New York City in November 2019, and a virtual expert group meeting in October 2020.

As the partnership grew with service providers, the Initiative understood the increasing need for knowledge-sharing, in particular for smaller tech companies and microplatforms to have useful resources for understanding data preservation and disclosure in the cross-border context. In response to this, the Data Disclosure Framework (DDF) was developed in November 2020 under the auspices of the Global Initiative.

This document, the result of active and persistent engagement between the Initiative and service providers, aims to provide comprehensive knowledge on general practices developed by international service providers in handling overseas government requests for data.

However, this document is not meant to be legal advice, and it is to be clarified that companies should always first consult their lawyers/national business associations on whether they are legally allowed to respond to any overseas requests in their jurisdiction.

DDF highlights the need for compliance with the rule of law and the protection of international human rights. This document has sought to integrate the jurisprudence and documents produced by human rights mechanisms, most notably the Human Rights Committee (HRC) monitoring the implementation of the International Covenant on Civil and Political Rights (ICCPR). It includes jurisprudence retrieved from the Universal Human Rights

Index (UHRI) database developed by the United Nations Office of the High Commissioner for Human Rights (OHCHR), as well as relevant concerns submitted to the Global Initiative by Ms. Fionnuala Ní Aoláin, Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism.

CHAPTER 1. INTRODUCTION

1.1 PURPOSE OF THE DATA DISCLOSURE FRAMEWORK

The purpose of the Data Disclosure Framework (DDF) is to assist smaller tech companies and microplatforms in understanding the widely observed concepts on data processing for law enforcement and criminal justice purposes, such as data preservation and disclosure, in the cross-border context.

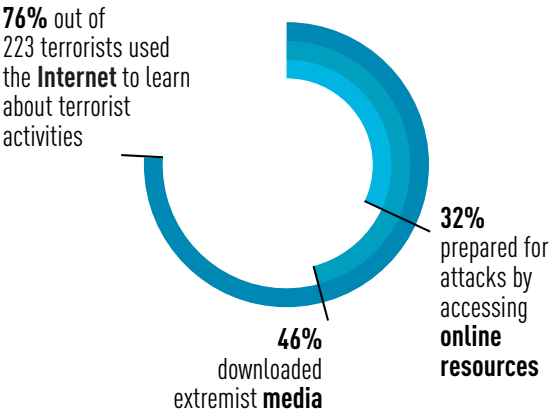
This increased understanding in turn ensures that such Internet/communications service providers (SPs) have the confidence to respond lawfully and speedily to requests for electronic evidence (e-evidence) in counter-terrorism investigations in a manner that is respectful of fundamental human rights including the right to privacy and freedom of expression.

While DDF may help with understanding basic concepts and technical knowledge, it must be noted that specific legislation and regulations for handling data and e-evidence vary between jurisdictions. SPs are responsible for checking whether their actions are lawful in their own jurisdiction, and under any applicable foreign laws.

1.2 CONTEXT

Use of the Internet is growing exponentially, with more than 4.57 billion users worldwide, which accounts for almost 47 per cent of the global population.[3] This rapid growth of use of the Internet is matched by an increase in criminal activity online. Upwards of 80 per cent of cyber-crime acts are thought to originate in some form of organized crime with online black markets, computer infection and harvesting of personal and financial data. It is estimated that the cost of cybercrime could reach US$5.2 trillion globally by 2023.[4] The Security Council in its resolution 2396 (2017) noted with concern "that terrorists craft distorted narratives, which are utilized to polarize communities, recruit supporters and foreign terrorist fighters, mobilize resources and garner support from sympathizers, in particular by exploiting information and communications technologies, including through the Internet and social media".

For example, a study entitled "What are the Roles of the Internet in Terrorism? Measuring Online Behaviors of Convicted UK Terrorists"[5] found that:



E-evidence can be important to show investigators where a suspect is located, who they are associating with and what they are communicating.

This is supported by a European Union survey[6] that shows that:

- E-evidence in any form is relevant in around 85 per cent of total (criminal) investigations
- In almost two thirds (65 per cent) of the investigations where e-evidence is relevant, a request to SPs based in another country is needed

The Report of the Secretary General on Small Arms and Light Weapons (S/2019/1011) also highlighted the increased use of the Internet for trade in firearms among unauthorized users,

[3] www.statista.com/statistics/617136/digital-population-worldwide/ 7 September 2020
[4] www.weforum.org/agenda/2019/11/cost-cybercrime-cybersecurity/
[5] www.voxpol.eu/download/vox-pol_publication/What-are-the-Roles-of-the-Internet-in-Terrorism.pdf.
[6] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0118&from=EN p.14.

including terrorist groups and transnational organized crime groups. The links between terrorism and organized crime include trafficking in arms, drugs, cultural property and trafficking in persons.The illicit trade in natural resources, transnational organized crime at sea and corruption were also further highlighted by Security Council resolution 2482 (2019).

When law enforcement and criminal justice officials identify electronic data in a foreign jurisdiction that has the potential to become e-evidence, the majority of cases would require invoking a mutual legal assistance (MLA) treaty, which can be complex and, in some States, bureaucratic, often resulting in lengthy delays in securing e-evidence. This does not resonate with the rapid nature of cyber- and transborder crime, where the Internet has no borders. Recent terrorist attacks have demonstrated the need for immediate responses to emergency incidents, preservation of data, as well as urgent requests for international cooperation.

To tackle these issues, the Global Initiative, launched by the UNODC, CTED and IAP to strengthen the capacity of law enforcement and criminal justice officials, held three expert group meetings from 2018 to 2020. The outcome of these three meetings was a "Practical Guide for Requesting Electronic Evidence Across Borders" (the "Practical Guide"), introducing best practices to strengthen the capacity of central authorities, prosecutors and law enforcement personnel regarding the most up-to-date procedures for requesting electronic evidence in counter-terrorism cases.

After the above process, the draft DDF was produced as a twin document of the Practical Guide. Compared to the Practical Guide, the draft DDF did not contain sensitive investigatory information but featured other types of information that may be more useful for SPs. A milestone virtual expert group meeting took place in October 2020 in the exclusive presence of SPs to examine the applicability and scalability of the draft DDF in their day-to-day operations. As a follow-up to this meeting, two expert groups were formed to amplify specific operational knowledge resulting in this first edition of DDF.

As transborder crime increases and potential e-evidence is routinely located across borders, DDF will equip SPs who are relatively new to this topic with an introductory reference for e-evidence.

Case study: Mark Taylor

A New Zealand jihadi fighting for ISIS tweeted his location from within the Syrian Arab Republic as he updated his followers on his time in the warzone. Mark Taylor, who is known on Twitter as @M_Taylor_Kiwi did not switch off the geolocation on his tweets as he travelled across the Syrian Arab Republic. Taylor, who changed his name to Abu Abdul-Rahman, made a series of 45 tweets which broadcast his ever-changing location. This could provide invaluable e-evidence to demonstrate his allegiance to ISIS and confirm strategic locations.[a]

[a] www.nzherald.co.nz/nz/kiwi-jihadist-calls-for-anzac-day-terror/GXVDGFE4GKYP5DY5RQCBJHACNU/

1.3 GENERAL PRACTICES

1.3.1 Roles and responsibilities

Competent State authorities for requesting e-evidence ("State authorities"), which may include law enforcement, prosecution, judiciary and/or central authority depending on the jurisdiction, have responsibilities to secure and handle e-evidence, while ensuring the validity and accuracy of their requests and their compliance with international human rights laws. Their judicial system will determine whether the disclosed data can be admissible as e-evidence in criminal proceedings. While practices vary among Member States, different practitioners may share roles; for example, in some jurisdictions law enforcement, prosecutors and judicial authorities may all make a direct request to foreign SPs.

It is critical that SPs receive clear and efficient data preservation and disclosure requests and respond appropriately. As a twin document of DDF, the Practical Guide serves as the main reference when UNODC provides technical assistance to Member States to strengthen the capacity of State authorities for handling e-evidence. The Practical Guide offers a comprehensive mapping of SPs, which includes both the contact information and law enforcement procedures taken from the official websites of SPs or any relevant open-source information. Some SPs voluntarily contributed their policy information through the Global Initiative to improve the quality of their interactions with overseas State authorities in the law enforcement response process.

Depending on the jurisdiction, some SPs may receive requests from overseas State authorities for preservation, and possibly also voluntary disclosure. For the requests falling under the mutual legal assistance (MLA) category, SPs will be in a position to cooperate with the appropriate authorities of local jurisdiction.

SPs are responsible for checking that every action related to data disclosure is in line with applicable law.

1.3.2 Scope of e-evidence

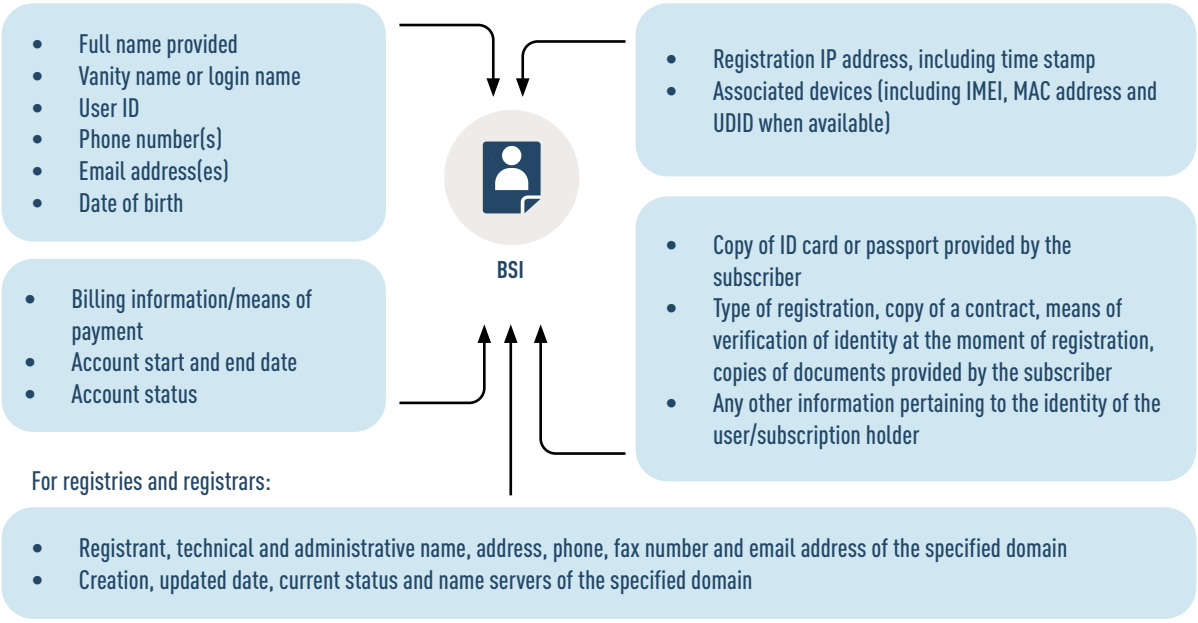
DDF will only consider electronically stored data, which are often divided into three categories: basic subscriber information (BSI), traffic and content data.

There are no internationally agreed definitions for the scope and categories of e-evidence and the modalities vary depending on the jurisdiction of the case, in particular the IP addresses (whether static or dynamic) and precise geo-location. The domain names registries and registrars may retain WHOIS data as identifying and contact information of their registrants.[7] This may include name, address, email, phone number, and administrative and technical contacts. The WHOIS data can be a form of stored e-evidence and is commonly considered as the basic subscriber information.

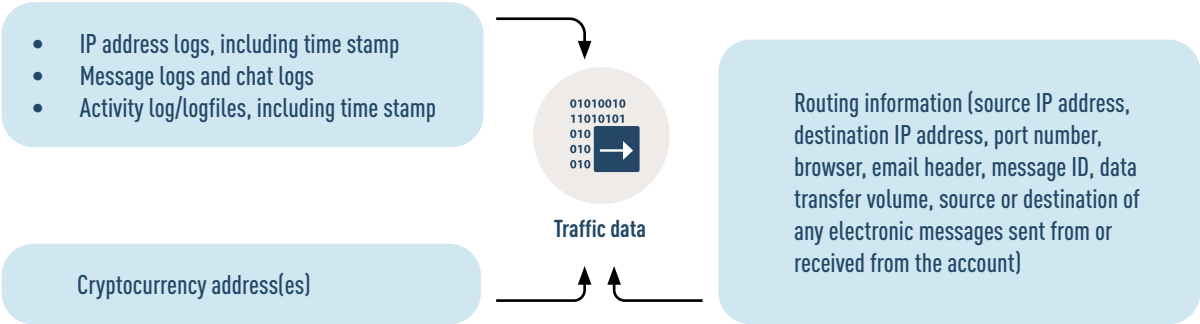
The following charts are useful in understanding commonly observed concepts for BSI, traffic and content data. SPs are responsible for checking how their operational environment and jurisdiction define the scope of potential e-evidence to avoid any breaches of laws. Also, local judicial systems will determine whether the processed data would become admissible evidence or not.

[7] See: https://whois.icann.org/en/about-whois

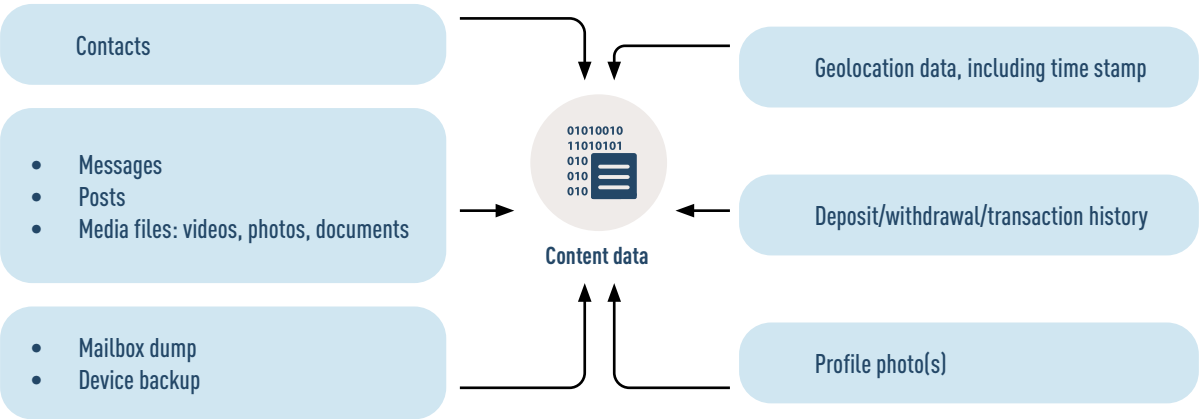
BSI: data sets from model forms



Traffic data: data sets from model forms



Content data: data sets from model forms



An example of raw message format of an email showing stored e-evidence:

```
Return-Path: <FShaker1234@us.sp.com>

Received: from [10.134.7.26] (34-277-761-341.cust-83.exponent-e.net. [34-277-761-
By smtp.us.sp.com with ESMTPSA id u22sm7299292999wrf.86.2019.02.15.09.53.07
For: <TMover1234@ca.sp.com>
(version=TLS1_2 cipher=ECDHE_RSA_AES128-GCM-SHA256 bits=128/128
Wed, 14 Feb 2018 09:54:06 -0800 (PST)
From: Felix Shaker <FShaker1234@us.sp.com>
Content-Type: multipart/alternative; boundary=us.com-mail-C6E76
5T87FES8V25
Content-Transfer-Encoding: 7bit
Mime-Version: 1.0 (1.o)
Date: Wed, 14 Feb 2018 17:54:06 +0000
Subject: Hello
Message-Id: <F5T08U61-76F6-5DN-94U8-V40654GH88FB@us.sp.co
References: <G7K07H51-87H9-6CX-06Gu-B73515HB92CR@ca.sp.co
<HT7PRO08VF80758C704R90U08T7FR8F609E0F50@AM8PRO7MB3075.eu
In-Reply-To: <HT7PRO08VF80758C704R90U08T7FR8F609E0F50@AM8PRO7MB3075.eurprd08.prod
To: Tahir Mover <TMover1234@ca.sp.com>
x-mailer: us.com Mail (15T70)
---us.com-mail- C6E76S65-8G09-404R-5G10-5T87FES8V25
Content-Type: text/plain; charset=utf-9
Content-Transfer-Encoding: quoted-printable
Hi Tahir,

I hope you are well
```

Traffic data (metadata): IP address showing where the email was sent from

Traffic data (metadata): Who sent the email – BSI from the SP could confirm more information on Felix Shaker

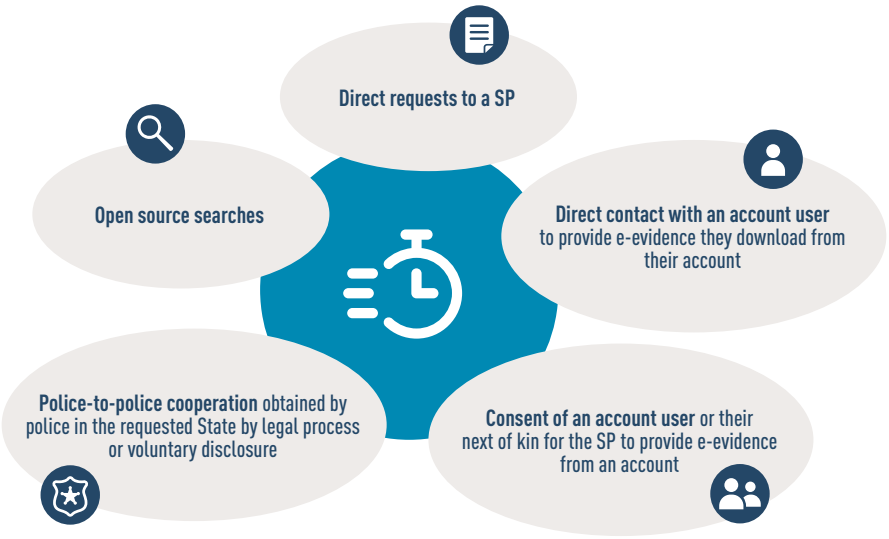
Traffic data (metadata): When the email was sent

Content data: Subject line

Traffic data (metadata): Who the email was sent to

Content data: Email message

There are different ways to obtain e-evidence for overseas State authorities. While mutual legal assistance is still widely used, the following actions can be taken during the investigation process.



Among the above actions, direct requests to an SP will be explained in detail in chapter 5. The possible interactions between SPs and users are elaborated in chapter 2. Since the target audience of DDF is SPs, the document does not cover open-source searches, joint investigation teams or direct interactions between State authorities and users.

Furthermore, DDF does not focus on covert online investigations and the moderation and takedowns of electronically stored or livestreaming content, as these have different dynamics and may go beyond the general practices presented in this document.

Model scenario:

Law enforcement officers are investigating the use of a cross-platform instant messaging app used by suspected terrorists to plan an attack. The law enforcement officers need the traffic data from the SP to locate where messages were sent from and then identify the unknown users believed to be part of the terrorist network. After receiving the live transmission of the real-time collection of available traffic data, law enforcement officers can identify those sending the messages and make arrests.

1.3.3 Law enforcement guidelines offered by service providers

SPs can voluntarily support the effort in two ways:

- Clearly indicating their contact information on their official website
- Publishing their law enforcement guidelines on their official website

Many SPs publish their procedures for preserving and requesting data in their law enforcement guidelines. The guidelines may provide the following information for overseas State authorities:

- Contact information to send requests and to serve legal process
- Preservation procedure
- Whether the SP discloses any data voluntarily and the procedures, for example, user consent, next-of-kin consent, user download or direct request for BSI and/or traffic data
- An emergency disclosure request procedure confirming if an SP has its own specific form for completion by law enforcement and specific requirements for disclosure

This document provides references to some model SP law enforcement guidelines in annex I. Also, click here for access to a website listing the contact information of SPs in the United States and available law enforcement guidelines.

1.4 USEFUL RESOURCES

The following resources on international cooperation in criminal matters are published for criminal justice officials but may also assist SPs in understanding the relevant concepts:

- Compendium of United Nations standards and norms in crime prevention and criminal justice, 2006
- Manual on International Cooperation in Criminal Matters related to Terrorism, 2009
- Revised Manuals on the Model Treaty on Extradition and on the Model Treaty on Mutual Assistance in Criminal Matters
- Model Law on Mutual Legal Assistance in Criminal Matters, 2007
- Model Treaty on Mutual Assistance in Criminal Matters, 1998

SPs may also wish to consult the following databases:

- Electronic Evidence Hub and Database of Legislation at the Sharing Electronic Resources and Laws on Crime (SHERLOC)
- UNIDIR Cyber Policy Portal

The following external resources are also useful to understand trends, commonly observed concepts and challenges related to e-evidence:

- Toolkit on Cross-Border Access to Electronic Evidence, Internet & Jurisdiction Policy Network, 2021
- Sirius EU Digital Evidence Situation Report - second Annual Report, EU SIRIUS, 2020
- Common challenges in combating cybercrime: As identified by Eurojust and Europol, Europol and Eurojust, 2019
- Internet & Jurisdiction Global Status Report, Internet & Jurisdiction Policy Network, 2019
- Commission Staff Working Document Impact Assessment (SWD/2018/118 final), European Commission, 2018

CHAPTER 2.
THE RIGHTS OF USERS

2.1 HUMAN RIGHTS AND DATA PROCESSING

2.1.1 United Nations and international legal standards

DDF has been drafted to ensure that this sub-initiative is consistent with international law, including international human rights law, in particular the rights to privacy, freedom of expression, non-discrimination and the right to due process of law. This means handling e-evidence by all involved parties must:

- Be necessary to support the prosecution of a perpetrator of a crime or to prove the innocence of a suspect and proportional to those ends
- Consider the impact on third parties and prevent intrusion on the private communications of those not subject to investigation
- Be subject to systems of independent oversight, both by judicial mechanisms as well as by other bodies mandated to ensure the lawful conduct of law enforcement and intelligence agencies
- Be lawful according to the laws and procedures of the requesting and requested States and in accordance with their international human rights obligations notably those arising from the United Nations International Covenant on Civil and Political Rights (ICCPR) and documents issued by the Human Rights Committee (HRC)
- Respect all human rights, in particular:

Human rights are universal, inalienable, indivisible and interdependent. However, in the context of requesting e-evidence across borders, it is imperative to uphold the protection and respect of the right to privacy and data protection by ensuring that personal data is collected, held, processed, used, transferred and disclosed in a manner that protects the privacy of individuals.

Other human rights particularly relevant to requests for e-evidence across borders are the rights to a fair trial, the recognition of a person before the law, non-discrimination, reputation, freedom of opinion and expression, freedom of association, freedom of movement and freedom of religion or belief.

In this respect, it is important to recall that any infringement on the right to privacy must comply with the principles of necessity and proportionality as well as non-discrimination. Any international transfer of personal information should be essential to the objective of the investigation and described in such a way as to prevent disclosure of data that is not strictly relevant, or necessary.

Generally, international human rights law sets a foundation for fundamental standards, and national laws protecting human rights vary from country to country. Thus, it is advisable, when in doubt, to always consult with the relevant authority of the requested State with regard to the conduct at issue.

The United Nations Human Rights Council has underlined the following human rights considerations, when reviewing the implementation by States parties of ICCPR.[8]

ICCPR article 17 (Right to privacy)

Ensure that national legislation is harmonized with ICCPR article 17, notably, legislation enshrining blanket data retention regimes for all telecommunication service providers or wide scope extended police powers.

Ensure that any interference with the right to privacy, with the family, with the home or with correspondence is authorized by laws that are publicly accessible; contain provisions that ensure that collection of, access to and use of communications data are tailored to specific legitimate aims; are sufficiently precise and specify in detail the precise circumstances and procedures for the use and storage of data collected.

Sufficient safeguards

Adequate safeguards against unnecessary and disproportionate interference with privacy of individuals in the context of online interception and surveillance, including data mining and large-scale interception of bulk telecommunications data, hacking and file decryption by the State security and intelligence services.

Institutional safeguards that spell out the conditions under which, if at all, data can be shared with foreign intelligence services, including independent oversight mechanisms and judicial involvement in the authorization of such measures; effective safeguards to the right of defence, including, if applicable, the opportunity to investigate and challenge the reliability of electronic data use as a source of evidence in a criminal case.

Procedural safeguards to notify victims whose right to privacy has been infringed through State-authorized surveillance activities about the infringement and provide them with an effective remedy in case of abuse.

Safeguards put in place against unwarranted and excessive interference with the right to privacy as well as steps taken to increase the transparency and independent oversight of surveillance systems.

[8] For more information, see the following HRC documents available at: https://uhri.ohchr.org/en/search-human-rights-recommendations CCPR/C/EST/CO/4 (CCPR 2019), CCPR/C/EST/CO/4 (CCPR 2019), CCPR/C/NOR/CO/7 (CCPR 2018), CCPR/C/PAK/CO/1 (CCPR 2017), CCPR/C/CHE/CO/4 (CCPR 2017), CCPR/C/ZAF/CO/1 (CCPR 2016), CCPR/C/GBR/CO/7 (CCPR 2015), CCPR/C/GBR/CO/7 (CCPR 2015), CCPR/C/GBR/CO/7 (CCPR 2015)

Even without unveiling the content, large portions of data about private communications may still provide information about one's behaviour, social relationships, private preferences and identity. Measures consisting in intercepting, collecting and retaining information of this nature may interfere with someone's right to privacy and are subject to the same protections outlined above.

2.1.2 Useful resources on human rights

Information relevant to considering the distinction between the criminal offence of incitement to acts of terrorism and the right to freedom of expression and privacy is available in the following resources of the United Nations:

Human rights and counter-terrorism:

- UNODC, The Module on Human Rights and Criminal Justice Responses to Terrorism of the Counter Terrorism Legal Training Curriculum, 2014, Section 2.3
- United Nations OHCHR, Human Rights, Terrorism and Counter-terrorism, Fact Sheet No. 32, 2008, chapter III, Section H and J
- United Nations Counter-Terrorism Implementation Task Force, Guidance to States on Human Rights-Compliant Responses to the Threat Posed by Foreign Fighters, chapters VII and X
- Reports of the United Nations Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: List

Human rights, including the right to privacy:

- General Assembly resolution A/RES/68/167, adopted on 21 January 2014
- United Nations OHCHR – The International Bill of Human Rights[9]
- ICCPR Status of Ratification – Interactive Dashboard[10]
- HRC General Comments No. 5 - Derogations, No. 13 -Administration of Justice,[11] No. 16 – Right to Privacy,[12] No. 29 -States of Emergency[13] and No. 32 – Right to a Fair Trial[14]
- Report of the United Nations OHCHR, The right to privacy in the digital age (A/HRC/27/37), adopted on 30 June 2014; also see General Assembly resolution A/RES/75/176 of 16 December 2020
- Reports of the United Nations Special Rapporteur on the right to privacy: List

Human rights and business:

- United Nations Global Compact, the Ten Principles of the United Nations Global Compact, Principles 1 and 2
- United Nations Guiding Principles on Business and Human Rights

Also consider the following important human rights aspects:

- Differing definitions of terrorism and risks of vague or overbroad definitions in legislation which are prone to arbitrary or even abusive application of counter-terrorism laws against people who are peacefully expressing dissenting views, human rights defenders, opposition activists or journalists
- Data protection principles (fair and lawful collection and processing of personal data, purpose specifications, access controls, protection for unauthorized access, limitations on transborder data flow, limited retention period, etc.)

[9] www.ohchr.org/EN/ProfessionalInterest/Pages/CoreInstruments.aspx
[10] https://indicators.ohchr.org/
[11] https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=INT%2fCCPR%2fGEC%2f4721&Lang=en
[12] https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=INT%2fCCPR%2fGEC%2f6624&Lang=en
[13] https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2f21%2fRev.1%2fAdd.11&Lang=en
[14] https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2fGC%2f32&Lang=en

- Risks of collusion/complicity in human rights violations by sharing information/evidence with other States where this information/evidence may be used in contravention of human rights standards

2.1.3 Preservation, data retention and data protection

The General Assembly stated that the same rights that people have offline must also be protected online. Data protection principles or legislation in some States limit data retention and are an essential component of the right to privacy (although data protection has been emerging as a distinct human or fundamental right).

Data retention is generally seen as a contravention of the principle of data minimization. In the European Union, for example, data minimization is defined in article 5(1)(c) of the General Data Protection Regulation (GDPR): "Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation)." Preservation of e-evidence is different to data retention, as the former relates to a targeted request to preserve the data of a specific user under criminal investigation (see chapter 3).

Data retention is the minimum or maximum periods of time an SP may be mandated by law to maintain data. This can assist a requesting State in knowing if an SP may have the data so it can be preserved pending a legal order to produce the e-evidence. Annex V provides a summary of data retention obligations for selected States. Data that continues to be preserved should, in most cases, be retained after data retention laws ordinarily permit or mandate its deletion.

There are no mandatory data retention rules in the United States. Nor do they exist at the European Union level, since the Data Retention Directive[15] was declared invalid by the European Court of Justice in 2014.[16] At the same time, data minimization requirements force SPs to delete data more quickly. This contributes to the volatility of e-evidence and results in less data being available for shorter periods of time, making the need for immediate preservation even more important.[17]

Practical note:

European Union users under the General Data Protection Regulation have the right to know exactly what data an SP is storing, obtain a copy of it, and have it deleted if they ask. A similar right is also found in many other data protection laws outside the European Union.

[15] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

[16] ECLI:EU:C:2014:238 (case C-293/12, *Digital Rights Ireland Ltd v. Minister for Communications*) and The Tele2/Watson case of December 2016, ECLI:EU:C:2016:970 (case C-203/15, Tele 2 Sverige).

[17] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0118&from=EN p.20.

Practical note:

Article 5 of GDPR requires that SPs only process personal data that is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. In other words, GDPR requires that SPs minimize their processing of personal data to the extent possible, which often requires SPs to refrain from retaining this data for unduly long periods. In addition, the Court of Justice of the European Union has repeatedly clarified that only targeted preservation requests are in accordance with European Union fundamental rights.

Therefore, any preservation request to an SP in the European Union must be limited with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period as is necessary for the prosecution of a specific crime.[a]

Many SPs offer a brief defined additional data retention period upon request where law enforcement makes a specific request for preservation. Considering the above, it is important for State authorities to explain in the initial request to the SP a reasonable duration period, and if possible, to explain the need for the requested identification period.

[a] See CJEU 6 October 2020, Case C-623/17, Privacy International, and in Joined Cases C-511/18, La Quadrature du Net and Others, C-512/18, French Data Network and Others, and C-520/18, Ordre des barreaux francophones et germanophone and Others at https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-10/cp200123en.pdf; and also CJEU 21 December 2016, Joined Cases C-203/15, Tele2 Sverige AB v. Post- och telestyrelsen, and C-698/15, *Secretary of State for the Home Department v. Tom Watson, Peter Brice, Geoffrey Lewis* at https://curia.europa.eu/juris/liste.jsf?num=C-203/15.

2.1.4 General Data Protection Regulation

"Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)"[18] entered into force on 24 May 2016 and has applied since 25 May 2018. For more information on the General Data Protection Regulation (GDPR), see the **European Commission website** and the **GDPR.EU website**.

While the scope of GDPR is focused on SPs providing services within the European Union, it also serves as the most commonly observed global data protection benchmark for SPs offering international services. This is due to the fact that GDPR provides one of the highest standards for data protection: compliance with GDPR often establishes a good starting point for further compliance with data protection legislation in other States. More and more SPs outside the European Union are voluntarily setting up their internal policies in line with GDPR, hoping their business grows in the European Union market while avoiding having too diverse internal policies in different States.

The core data protection principles outlined in article 5 of GDPR are popularly used by SPs:

Personal data shall be:

(a) Processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

(b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving

[18] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

(f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

Processing of data under General Data Protection Regulation

For State authorities, the European Union General Data Protection Regulation (GDPR) article 2(2)(d), and recital (19) stipulate that it should not apply to the processing of personal data by competent authorities (i.e., law enforcement) for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security and the free movement of such data.[19]

Importantly for SPs, however, this does not stop GDPR from applying to the processing by private bodies that hold the personal data sought by competent authorities for these exempt activities. Further, that same recital (19) goes on to note that:

> When the processing of personal data by private bodies falls within the scope of this Regulation, this Regulation should provide for the possibility for Member States under specific conditions to restrict by law certain obligations and rights when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard specific important interests including public security and the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

Thus, individual European Union Member States may have different legal requirements in this field.

SPs are responsible for checking whether GDPR and domestic legislation permits the processing of the requested data – including transmitting it to domestic and overseas State authorities. Specifically, for GDPR, SPs may want to confirm if one of the specific grounds in article 6 is fulfilled and also the other principles in article 5 are complied with, examining whether a foreign order is sufficient legal grounds for processing data.

[19] Those activities are instead regulated by the Directive (EU) 2016/680 establishing rules for the protection of individuals with regard to the processing of personal data by competent authorities for purposes of law enforcement.

The following is article 6(1) of GDPR:[20]

> Processing shall be lawful only if and to the extent that at least one of the following applies:
>
> (a) The data subject has given consent to the processing of his or her personal data for one or more specific purposes;
>
> (b) Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
>
> (c) Processing is necessary for compliance with a legal obligation to which the controller is subject;
>
> (d) Processing is necessary in order to protect the vital interests of the data subject or of another natural person;
>
> (e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
>
> (f) Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.
>
> Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

Further, where user data is directly transmitted to an overseas State authority, the conditions of GDPR on transfers of personal data to a third country must be complied with, which in general require that either an adequacy decision by the European Union Commission for the State, or that other appropriate safeguards are in place, such as an international agreement regulating such transfers. See chapter 6.3 for more information.

Resources on European Union data protection law including GDPR:

- Handbook on European Data Protection Law - 2018 edition
- Complete Guidance to GDPR Compliance, GDPR. European Union official website including GDPR checklist
- Data Protection in the EU, European Commission website

2.1.5 Other examples of data protection and privacy legislations

Personal Information Protection and Electronic Documents Act

In Canada, the Personal Information and Electronic Documents Act (PIPEDA) applies to all private sector SPs that operate in Canada, and process personal information about individuals in Canada. PIPEDA includes many general requirements governing how and when SPs may disclose personal information. Relevant here, PIPEDA generally prevents the disclosure of personal information without consent from the data subject, except in certain situations, including:

1) when disclosure is "required to comply with a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel the production of information, or to comply with rules of court relating to the production of records;" and
2) when disclosure "is requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement

[20] See the full article 6 at: https://gdpr.eu/article-6-how-to-process-personal-data-legally/.

of any such law or gathering intelligence for the purpose of enforcing any such law."[21]

Additionally, Canada has currently proposed legislation, referred to as the Consumer Privacy Protection Act, which would replace PIPEDA. Even if it does so, it still includes similar restrictions on the ability of SPs to disclose information to requesting State authorities.

The California Consumer Privacy Act

The California Consumer Privacy Act (CCPA) is a state statute which entered into force on 1 January 2020 in California State in the United States. The California Privacy Rights Act was also passed in November 2020, building upon the existing CCPA.

CCPA is intended to empower user control over the personal information collected by SPs and its regulations provide guidance on implementation. The CCPA sets a foundation for the following four core privacy rights:

- The right to know about the personal information a business collects about them and how it is used and shared
- The right to delete personal information collected from them (with some exceptions)
- The right to opt-out of the sale of their personal information
- The right to non-discrimination for exercising their CCPA rights[22]

2.2 USER CONTROL OVER THEIR DATA

2.2.1 User consent

In many jurisdictions, SPs can disclose any data if they receive consent from the user.[23] The user can then decide if they share the content with the authorities in their State. It will be important to ensure that consent has been provided of the user's freewill. This may require an independent witness to verify the consent or to have notarized consent. For example, Apple will provide content in response to user/customer consent within the United States.[24]

Deceased users

There may also be occasions where the next-of-kin request access to a user's account.

Facebook and Instagram offer two options: to delete the account or to memorialize the account. Users are able to decide in advance or nominate someone to be a "legacy contact" who can manage the account. According to Facebook's privacy rules, the legacy contact cannot see private messages.[25]

Case study

In July 2018, the Federal Court of Justice of Germany ruled that social media accounts are no different than personal letters and diaries and can be inherited.[a]

[a] http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=pm&Datum=2018&Sort=3&nr=85390&pos=0&anz=115.

[21] See "Disclosure without knowledge or consent" at https://laws-lois.justice.gc.ca/eng/acts/p-8.6/page-2.html.
[22] More information available at: https://oag.ca.gov/privacy/ccpa.
[23] Examples: see the Electronic Communications Privacy Act of 1986 (ECPA) § 2702(b)(3); PIPEDA § 7(3).
[24] www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf.
[25] www.facebook.com/help/1568013990080948?helpref=faq_content.

2.2.2 User download

Another effective tool is to allow a user access their own content, for example:

- Facebook users can download their account content such as messages, photos, videos and wall posts.[26]
- Google Takeout allows users of Google products, such as YouTube and Gmail, to export their data to a downloadable ZIP file.[27]
- Twitter users can obtain a download of Tweets posted to their account.[28]
- Apple users can get a copy of the data associated with their Apple ID, such as sign-in, iCloud and purchase activities.[29]

2.3 USER NOTIFICATION

When preserving data following a legal request, SPs may need to check if their technical design or operational policy addresses any notification to the concerned user (user notification). Documents such as compulsory non-disclosure or gag orders stipulating that users are not to be informed of data processing do not necessarily accompany requests in the context of cross-border preservation and disclosure.

Thus, the decision on user notification on data processing requires careful application of the necessity and proportionality principles. If an investigation is overt, sending a notification can help the user to prepare for a fair trial. If the user is under covert investigations, alarming the suspect of an e-evidence request could jeopardize ongoing investigations and could increase security threats against victims in serious cases. Referring to the local operational environment is a good first step. Many States provide legislation or rules on the waiver of user notification on exceptional grounds, including covert investigations.

In all cases, SPs may wish to avoid any critical harm to ongoing criminal investigations, to the extent permissible under law. If the technical design or operational policy of an SP requires user notification by deciding to preserve or disclose the data, or if it is legally required to do so, the SP can directly communicate such implications to requesters before taking any further action. The requesters will then decide whether they would risk a notification and seek the data, or strictly avoid such cases and find another way of cooperation such as mutual legal assitance.

If an SP would like to have some flexibility in this regard and increase the space of assessment, they could consider:

- A technical design which gives control on user notification, so this is not automatic, to the extent permitted by law
- A policy to determine in which circumstances non-notification to users of law enforcement requests for preservation and disclosure is justifiable, if permitted by law

The following may assist in the formulation of any notification policy:

- If an investigation is overt, for example, the user has been arrested, the risk of destruction of evidence, alerting other persons of interest and evading justice are reduced by an SP notifying the user of the preservation request
- If an investigation is covert and a user is unaware of an ongoing investigation, notification is delayed to prevent:
  - Destruction of evidence
  - Alerting other persons of interest
  - Persons evading justice
  - Creating risks to, for example, witnesses or victims

[26] www.facebook.com/help/1701730696756992.
[27] https://support.google.com/accounts/answer/3024190?hl=en.
[28] https://help.twitter.com/en/managing-your-account/how-to-download-your-twitter-archive.
[29] https://support.apple.com/en-us/HT208502.

Different SPs have different policies on user notification. If an overseas State authority requests data preservation or disclosure by SPs in the United States, prevailing SP policy is not to notify the user and the e-evidence request remains confidential. In the European Union, practices may vary depending on local legislation, while GDPR does not provide any specific or exceptional clauses on the preservation of data for criminal investigation purposes.

For example, Twitter's policy is to notify users of requests for their account information, which includes a copy of the request, prior to or after disclosure unless prohibited. Twitter requires that if user notice is prohibited, the basis must be included in any direct request and for a specific duration, and this can include terrorism investigations.[30]

When requested not to notify

State authorities will routinely include a paragraph not to notify a user if this will impact the investigation. This must be justified with specific reasons as to why user notification would have an impact on the investigation. For example, notifying the user will alert them of a covert investigation and lead to destruction of e-evidence. It is recommended that this be made explicit in the law enforcement guidelines of SPs.

An example paragraph requesting non-disclosure could be the following:

> "I request that you do not disclose the existence of this request to the subscriber or any other person, other than as necessary to comply with this request. If compliance with this request might result in a permanent or temporary termination of service to the account(s), or otherwise alert any user of the account(s) as to your actions to preserve the information described below, please contact me as soon as possible and before taking action."

Case study: European Court of Human Rights

The principal position of the European Court of Human Rights on this issue is that the notification of people subject to surveillance measures, including disclosure of their data, is an essential precondition to allow affected individuals to exercise their rights and apply for remedies. As the law itself must provide for an obligation to notify the user, this duty should in general rest with the State authorities, although this is not elaborated in detail by the Court, because the most important aspect is that the individual gets notified. The Court also acknowledges that if a suspect is notified too early, this might endanger ongoing investigations. Notification should therefore be provided as soon as it would no longer jeopardize such investigations. Where this is not possible, for example, constant surveillance of suspected terrorists, etc., notification should at least be provided to an independent authority, which exercises the rights of the individual on his/her behalf until the individual can be notified.[a]

[a] See: *Klaas and Others v. Germany* (App. No 5029/71), *Leander v. Sweden* (App. No. 9248/81), *Weber and Saravia v. Germany* (App. No. 54934/00), *Association of European Integration and Human Rights and Ekimdzhiev v. Bulgaria* (App. No. 62540/00) and *Zakharov v. Russia* (App no 47143/06).

[30] See the section "Will Twitter notify users of requests for account information?" at: https://help.twitter.com/en/rules-and-policies/twitter-law-enforcement-support#10.

CHAPTER 3. PRESERVATION

3.1 BASIC CONCEPTS

Preservation is a "snapshot" of the entire user's account sought to be preserved at the time the request is received and processed by SPs. To ensure this process is quick to prevent deletion or a change in format by a user, State authorities may contact SPs to preserve data.

Preserving or freezing data is a fundamental step for State authorities to ensure that the requested data is available when they send a disclosure request. In some States, strong data protection obligations might prevent SPs from storing user's data for a long period. The data preservation for criminal investigation purposes often extends the data storing period beyond the usual standards, and overseas State authorities would be able to send a mutual legal assistance request in the expectation of producing the preserved e-evidence if the appropriate legal standards and other applicable laws in the requested State are met.

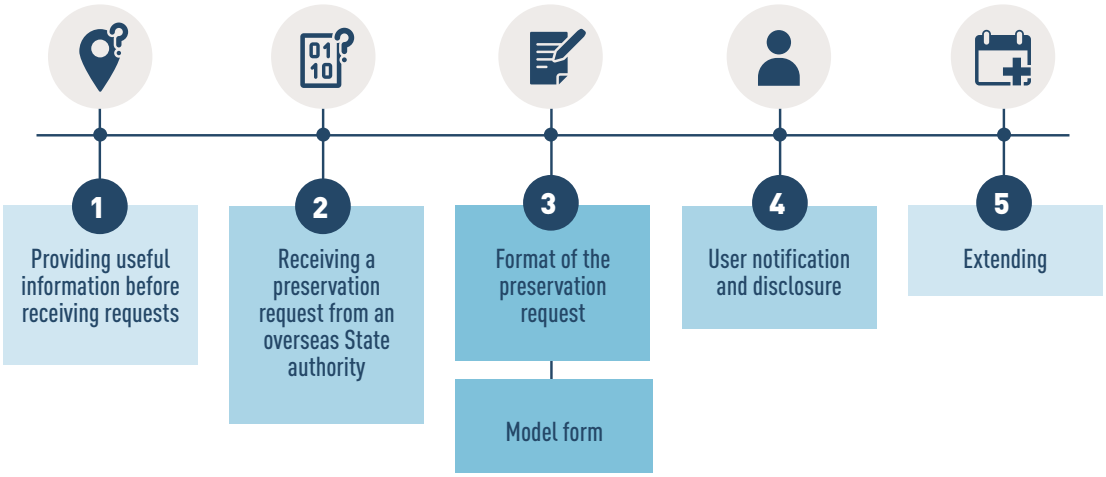
Member States have different legislation, regulations, rules and operational customs on data preservation, ranging from requiring a court order to an informal request. It is possible that some jurisdictions do not specifically prohibit overseas State authorities from making direct contact with SPs to request the preservation of data, since such an act alone does not automatically lead to data disclosure. On the other hand, data preservation already leads to data storage (processing) under GDPR. It is difficult to generalize all practices in various States, so SPs need to check their local operational environment and any other applicable laws to avoid any breach of laws.

In DDF, this chapter will mainly focus on cases where SPs are directly contacted by overseas State authorities for voluntary preservation. A "requesting State" refers to a State requesting data preservation and/or disclosure to a foreign SP.

Practical note: Police-to-police cooperation

Police in a requesting State may liaise with police in a requested State for preservation on its behalf. This can be a speedier route as law enforcement in the requested State should have greater expertise on the application of SP procedures as well as local legislation and regulations. For these reasons, SPs may receive a request from a law enforcement agency in their own jurisdiction, on behalf of another State.

3.2 PRESERVATION ESSENTIALS



3.2.1 Providing useful information before receiving requests

Data can be deleted or changed in format before SPs receive a preservation request from law enforcement. Some SPs store limited data for only a short period of time.[31]

Two examples are Snapchat and WhatsApp:

> "Generally, once a Snap has been opened by all recipients, the content is permanently deleted and unavailable. If a Snap is unopened by one or more recipients, it may remain on our servers for up to 30 days. A Snap that has been posted to a user's Story can be viewed for up to 24 hours. Typically, the posted Snap is permanently deleted and unavailable 24 hours after being posted to their Story. Chat content will typically only be available if the sender or recipient has chosen to save the Chat. Memories content may be available until deleted by a user."[32]

> "WhatsApp does not store messages once they are delivered or transaction logs of such delivered messages. Undelivered messages are deleted from our servers after 30 days."[33]

SPs also require different sets of information to identify a specific account.[34] The types of account identifier may depend on the technical design of the platform of the SP.

It would be practical for an SP to explain such useful information in their law enforcement guidelines for better communications. The following can be considered:

- Data retention periods and account identifier
- What data is available
- Where a request to preserve should be sent (usually to an SP email address)
- If the SP has a specific form that must be completed by a State authority
- State authorities to confirm their identity by sending any requests from an official email address
- How long e-evidence will be preserved for
- How to extend preservation until the e-evidence is lawfully produced

[31] See chapter 2.1.3 of this document on preservation, data retention and data protection.
[32] https://snap.com/en-US/safety/safety-enforcement
[33] https://faq.whatsapp.com/general/security-and-privacy/information-for-law-enforcement-authorities/?lang=en
[34] See the example of Kik at: www.kik.com/uploads/files/Kik%20Law%20Enforcement%20Guide-Final%202021.pdf, p.5.

3.2.2 Receiving a preservation request from an overseas State authority

An overseas State authority will contact SPs directly and request that data be kept in a native format as of the date of the request. Essentially this is a snapshot of the data, content and non-content, and is usually preserved until a valid and lawful request has been received for production. A preservation request should usually not concern the entire account, unless the circumstances can justify its necessity and proportionality.

SPs may have data stored in different parts of the world, but this does not mean that a preservation request should be sent to where the SP stores the data. The preservation request should be sent to the establishment or legal representation of the SP that is responsible for data preservation and disclosure. If an SP has published law enforcement guidelines, this information is usually specified.

Concerning user notification, which may have already taken place after data preservation in some cases, see chapter 2.3 of this document.

Practical note

INTERPOL recommends that Member States – if permitted in their legal system – appoint a national team of experts or single point of contact that can cooperate with SPs. This will prevent more than one agency applying for preservation if there are multiple investigations and will ensure the e-evidence is preserved expeditiously.

Practical note

Once the data is preserved, the SP can provide a reference number to the State authority making the request. This preservation reference number for the original preservation and any extension are often included in a court order and relevant communications, so the SP can quickly access the e-evidence again when needed.

3.2.3 Format of the preservation request

Some SPs have their own request form for preservation requests or have an online portal where a request can be completed. For example, Facebook preservation requests should be made through their law enforcement online request system.

SPs have complete autonomy to design the forms so they comply with the law and their technical design, contain the information needed to ensure speedy preservation, and justify retaining the data for law enforcement purposes. Any form should include as standard:

- Specific account identifiers to access the data quickly, confirming that a separate preservation request will be required for separate account identifiers
- What data must be preserved: BSI, traffic data or content data
- The relevance of the data to the criminal offences being investigated for law enforcement investigation. For example, the content data is requested to be preserved from account identifier xxx used to disseminate terrorist recruitment videos

SPs may also include in their preservation request form:

- Request to attach relevant screenshots to a preservation request to demonstrate the relevance of the account identifier to a criminal investigation

- Confirm the time frame for the data requested so the data preserved is specifically linked to the criminality being investigated, rather than to the entirety of the data in the account identifier which may not be linked to the criminality

If an SP does not have a specific form or portal, the model preservation request form enclosed as annex II could be helpful.

3.2.4 Extending

SPs can offer the extension of the data preservation period, within the extent that is permitted in applicable law. For example, Apple will preserve data for 90 days plus a 90-day extension.[35]

Case study: United States

United States law enforcement agencies can request SPs to preserve e-evidence for an initial period of 90 days, which can be extended for an additional 90-day period upon a renewed request. In relation to process, the Electronic Communications Privacy Act (ECPA)[a] provides that a preservation request is made by a law enforcement agency directly to the SP. A court order is not required.

ECPA does not refer to preservation requests from foreign law enforcement officers. The major SPs follow the ECPA 90 day plus 90-day extension periods (180 days total) for preservation requests from foreign law enforcement officers. A request to extend the preservation should be submitted to SPs by the overseas law enforcement agency before the expiry of the first 90 days.

[a] See 18 U.S.C. §2703(f) at: www.law.cornell.edu/uscode/text/18/2703.

[35] www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf and www.apple.com/legal/privacy/law-enforcement-guidelines-outside-us.pdf.

3.2.5 Model scenario

The model scenario below will assist with how this model preservation request form is used by an overseas State authority.

Model scenario;[a] The New Country Counter-Terrorism Police

A video has been posted to YouTube: Ground Zero: Syria (Part 7) – Snipers of Aleppo supporting the Al-Nusrah Front (ANF) – an alternative name for Al-Qaida. The New Country Counter-Terrorism Police Internet Referral Unit has been monitoring comments on the video and observed Victory4Mujahideen post on 15 December 2020: "Want to go for jihad Syria, email: Akan007@icloud.com" and "Allahu Akbar, I'm going as well insha'allah". Operation Improve is commenced to determine who has posted the comments and who the user is of Akan007@icloud.com and if it is connected to the ANF. The first stage is for the New Country Counter-Terrorism police to immediately preserve the account identifier Victory4Mujahideen with Google and email account Akan007@icloud.com with Apple to ensure the data is available for any direct request or mutual legal assistance request. After reviewing the Apple law enforcement guidelines, the New Country Counter-Terrorism Police draft the model preservation request form below to Apple.

[a] In considering the case scenario, it is important to recall that the Security Council has emphasized that terrorism cannot, and should not, be associated with any religion, nationality or civilization.

REQUEST FOR THE PRESERVATION OF ELECTRONIC DATA
Date: 15 December 2020

REQUESTING AUTHORITY: New Country Counter-Terrorism Police
Identification details:
- Full name or personal identification number: Inspector Nicked (DI390)
- Position held: Inspector of Police

Contact details of authority's representative:
Phone number: +123(0)2435 627348 Ext: 553336
Email: di.nicked@police.nc

Proceedings number: n/a

ADDRESSEE (RECIPIENT): Apple

Address: lawenforcement@apple.com

This authority is conducting a criminal investigation (Operation Improve) that involves users from your platform. Electronic data has been deemed relevant in this matter. I am hereby requesting your company to immediately take all necessary actions to preserve and safeguard electronic data in relation to the user(s) and/or account(s) mentioned below.

TYPE OF PRESERVATION REQUEST:
x New preservation request

NATURE OF THE CASE:
Click here to describe the nature of the crime investigated. Provide as much information and context as possible, in relation to this particular request for electronic data.
Examples of information that may be provided here in addition to the nature of the case:
- *Status/progress (e.g., pre-arrest, pretrial, trial, crime in progress, ...)*
- *National criminal code article/law/statute defining the offence you are investigating*
- *Maximum sentence according to your national law*
- *Nationality or long-term residence if known*

The Internet Referral Unit (IRU) of the New Country Counter-Terrorism Police commenced the monitoring of a video on YouTube: Ground Zero: Syria (Part 7) - Snipers of Aleppo supporting the proscribed terrorist organization the Al-Nusrah Front. The IRU observed a comment posted by Victory4Mujahideen on 15 December 2020, stating, "Want to go for jihad

continued

Syria, email: Akan007@icloud.com" and "Allahu Akbar, I'm going as well insha'allah" Operation Improve has been commenced by the New Country Counter-Terrorism Police to determine the identity of Victory4Mujahideen and user Akan007@icloud.com and investigate the offences of encouraging terrorism in New Country contrary to section 4 of the Anti-Terrorism Act 2007, dissemination of terrorist material contrary to section 2(3) of the Anti-Terrorism Act 2007 and membership of a proscribed terrorist organization (ANF) contrary to section 5 Terrorism Act 2007.

LEGAL BASIS:
Lay down the legal basis under which the request is being made, according to domestic legislation.
Preservation of data related to a terrorism investigation pursuant to Anti-Terrorism Act 2007 section 21(4)

DOMESTIC LEGAL PROCESS:
If required by the service provider, attach the domestic legal process for the requested information to be preserved in accordance with legislation in your country.
Not required for a request to another State

CONCERNED USER OR ACCOUNT:
Click here to enter all the information available about the subject of the investigation, (such as name, email address, account ID, phone number, device information, domain name for registry/registrar, Bitcoin address, Bitcoin transactions, IP addresses, credit card or bank account), to assist the company in identifying the concerned accounts.
If possible, state if the subject is a suspect, victim, witness or person of interest in your investigation.
It is also advised to include screenshots and full URLs, if available.
Akan007@icloud.com
See Screenshot from 15 December 2020

DATA SETS:
This request applies to the items indicated below, whether in electronic or other form, including information stored on backup media, if available. A justification for the request for preservation of these data sets will follow.

Basic subscriber information
- Full name provided
- Vanity name or login name
- User ID
- Phone number(s)
- Email address(es)
- Date of birth
- Billing information/means of payment
- Account start and end date
- Account status
- Registration IP address, including time stamp
- Associated devices (including IMEI, MAC address and UDID when available)
- Copy of ID card or passport provided by the subscriber
- Type of registration, copy of a contract, means of verification of identity at the moment of registration, copies of documents provided by the subscriber
- Any other information pertaining to the identity of the user/subscription holder

Traffic data
- IP address logs, including time stamp
- Message logs and chat logs
- Activity log/logfiles, including time stamp
- Routing information (source IP address, destination IP address, port number, browser, email header, message ID, data transfer volume, source or destination of any electronic messages sent from or received from the account)

Content data
- Contacts
- Messages
- Posts
- Media files: videos, photos, documents
- Mailbox dump
- Device backup
- Geolocation data, including time stamp
- Deposit/withdrawal/transaction history
- Account balance
- Profile photo(s)

Other data: n/a

JUSTIFICATION, INCLUDING FOR NECESSITY AND PROPORTIONALITY:
Justify how the information to be preserved will assist in the investigation. If possible, make this justification for each specific piece of information requested above. Overbreadth is the most common reason companies give for refusal.
Operation Improve has commenced to determine the identity of account identifier Akan007@icloud.com after a post on an Al-Nusrah Front (ANF) video posted to YouTube: Ground Zero: Syria (Part 7) - Snipers of Aleppo. Account identifier Victory4Mujahideen posted a comment to the video on 15 December 2020: "Want to go for jihad Syria, email: Akan007@icloud.com" and "Allahu Akbar, I'm going as well insha'allah"

continued

Al-Qaida is a proscribed terrorist organization in New Country pursuant to Schedule One of the Anti-Terrorism Act 2007. The ANF should be treated as an alternative name for the organization which is already proscribed under the name Al-Qaida.

The basic subscriber information, traffic data and content data will also enable the New Country Counter-Terrorism Police to secure any evidence to support a prosecution for encouraging terrorism in New Country contrary to section 4 of the Anti-Terrorism Act 2007, dissemination of terrorist material contrary to section 2(3) of the Anti-Terrorism Act 2007 and membership of a proscribed terrorist organization (ANF) contrary to section 5 Terrorism Act 2007.

TIME RANGE/PERIOD:
Specify here the time frame of the information to be preserved. Provide a time frame that is as narrow as possible to avoid making overly broad requests and specify the time zone.
Spell out the month, instead of using the number, as date format is different in the United States.

The requested time frame is from the date of the receipt of the preservation request.

FOLLOW-UP:
X Formal judicial request for the disclosure of content data under international judicial cooperation to the United States for Akan007@icloud.com
X Direct request for voluntary disclosure of BSI and traffic data for Akan007@icloud.com
X Preservation request has been submitted to Google for user Victory4Mujahideen
X Direct request will be submitted to Google for BSI and traffic data for Victory4Mujahideen

CONFIDENTIALITY:
☒ I request that you do not disclose the existence of this request to the subscriber or any other person, other than as necessary to comply with this request. If compliance with this request might result in a permanent or temporary termination of service to the account(s), or otherwise alert any user of the account(s) as to your actions to disclose the information described below, please contact me as soon as possible before taking action

Click here to state the reasons why prohibition of notification to the user is requested. Specify the statute, if any, under which the non-disclosure request is being made. Please also include the end date of the user notice prohibition, if applicable.
If notice is prohibited to the subscriber, and you have obtained a domestic court order attach here.

As the identity of Victory4Mujahideen and Akan007@icloud.com are unknown, to notify the user of this preservation request would alert them and potentially other members of the terrorist organization Al-Qaida, of the nature and stage of the investigation. If this were a similar case in New Country a non-notification and non-disclosure order would be justified pursuant to section 32 of the Anti-Terrorism Act 2007.
Attach court order if available

PGP: *Attach PGP Public Key (if applicable)*

SUMMARY OF DOCUMENTS ATTACHED:
1. Screenshot of comments by Victory4Mujahideen on 15 December 2020
2. Relevant law under the Anti-Terrorism Act 2007: Sections 2(3), 4, 5, 21(4) and 32 and Schedule One

If you have questions regarding this request, please contact me.

I hereby certify I have the legal authority to submit this request and that the information provided is true to the best of my knowledge.

Before submitting this request, print, sign and stamp it. Then, scan and submit it to the company digitally, following their guidelines.

NEW COUNTRY POLICE

Apple confirms the preservation of email account Akan007@icloud.com for 90 days to 15 March 2021 with reference number: folio 0028 GCC-537199-N5S0D8.

The officer begins to consider taking steps towards requesting the e-evidence and makes a diary note for two weeks before the expiry of the preservation, on 1 March 2021, to extend the preservation for a further 90 days. This will prevent the e-evidence being deleted before any request or court order to produce the e-evidence has been received by the SP.

3.3 PRESERVATION REQUEST CHECKLIST

The following table could be a useful preservation request checklist.[36]

PRESERVATION REQUEST CHECKLIST				
Date and time preservation request received				
Who preservation request is received from				
SENDER				
Who sent the request:				
Law enforcement officer	☐	**Yes**	☐	**No**
Is the officer's name included?	☐	Yes	☐	No
Is the officer's rank included?	☐	Yes	☐	No
Has the officer confirmed they have the required legal authority to make the request?	☐	Yes	☐	No
Has the request been sent from an official email address?	☐	Yes	☐	No
Has the request been authorized by a senior officer?	☐	Yes	☐	No
Prosecutor	☐	**Yes**	☐	**No**
Is the prosecutor's name included?	☐	Yes	☐	No
Has the prosecutor confirmed they have the required legal authority to make the request?	☐	Yes	☐	No
Has the request been sent from an official email address?	☐	Yes	☐	No
Judicial authority	☐	**Yes**	☐	**No**
Is the judge's name included?	☐	Yes	☐	No
Has the judge confirmed they have the required legal authority to make the request?	☐	Yes	☐	No
Has the request been sent from an official email address?	☐	Yes	☐	No

[36] Available in PDF format at: https://sherloc.unodc.org/cld/en/st/evidence/ddf.html

PRESERVATION REQUEST CHECKLIST *(continued)*

ACCOUNT IDENTIFIER		
Has the correct identifier been provided to enable the data to be preserved?	☐ Yes	☐ No
CRIMINAL INVESTIGATION		
Have the criminal offences been listed?	☐ Yes	☐ No
Has confirmation been provided that the data to be preserved is linked to the investigation of these criminal offences?	☐ Yes	☐ No
DATA TO BE PRESERVED		
BSI?	☐ Yes	☐ No
Traffic data?	☐ Yes	☐ No
Content data?	☐ Yes	☐ No
TIMELINE		
Has a time frame been provided for the requested data?	☐ Yes	☐ No
CONFIDENTIALITY		
Is a paragraph included not to notify the user of the existence of the request?	☐ Yes	☐ No
Confirm – even in absence of request – that the user will not be notified through termination of service	☐ Yes	☐ No
CONFIRMATION		
Has the sender been notified the data has been preserved?	☐ Yes	☐ No
Has the sender been notified of the expiry date of the preservation?	☐ Yes	☐ No
Has the sender been notified of the preservation reference number?	☐ Yes	☐ No
If an extension request: Has the sender been notified of the date of extension?	☐ Yes	☐ No
Has the sender been notified of the expiry date of the extended preservation?	☐ Yes	☐ No

CHAPTER 4. CROSS-BORDER VOLUNTARY DISCLOSURE

4.1 BASIC CONCEPTS

Investigations and prosecutions requiring e-evidence can be sophisticated, complex and quick moving. To obtain e-evidence at the earliest opportunity, SPs may receive requests from overseas law enforcement for voluntary disclosure.

Each State determines according to its national law if the cross-border voluntary disclosure methods outlined below can be used and if SPs in its territory are allowed to communicate with or transfer data directly to overseas State authorities. SPs also need to bear in mind that legal definitions and the scope of data categories vary among different jurisdictions, and the request the SP received might not have been sufficiently adapted to the local operational environment of the SP. Content data, which is possible to disclose through formal procedures (such as MLA), is often restricted for voluntary disclosures due to privacy concerns.

SPs are encouraged to take careful consideration of necessity and proportionality principles before disclosing any data. SPs who receive overseas requests for voluntary disclosure and are uncertain of lawful actions may wish to contact responsible authorities in their jurisdiction, such as the central authorities or get further information from their local business associations. It is crucial that SPs check their own operational environment to ensure that SPs do not breach any laws or rules owing to their voluntary actions.

As of April 2021, it has been observed that a large number of United States SPs operate with unique practices on voluntary disclosure. This is also increasingly observed by Canadian SPs for emergency cases.

This chapter shows both non-emergency and emergency cases:

- **Non-emergency voluntary disclosure** provides information on conditions, choices and procedures to produce BSI and/or traffic data (i.e., non-content data) without MLA
- **Emergency disclosure** explains how a service provider would receive and respond to an emergency disclosure request to produce BSI, traffic data and content data through MLA to prevent death or serious harm to individuals

Case study

In Canada and the United States, the following legislation is commonly referred to when handling e-evidence:

Canada:

- Uniform Electronic Evidence Act (1998)
- Personal Information Protection and Electronic Documents Act (PIPEDA) of 2000

United States:

- Electronic Communications Privacy Act of 1986 (ECPA)
- Stored Communications Act (SCA) of 1986
- CLOUD Act of 2018
- In the State of California: California Consumer Privacy Act (CCPA) of 2018

4.2 HUMAN RIGHTS SAFEGUARDS

DDF strongly encourages that direct requests be handled in line with international human rights laws and the rule of law (due process). The Universal Declaration of Human Rights can be used as a reference before voluntarily disclosing any data, as it establishes the following fundamental human rights:[37]

- Article 3 on the right to life, liberty and security
- Article 5 on torture or to cruel, inhuman or degrading treatment or punishment
- Article 6 on recognition everywhere as a person before the law
- Article 7 on non-discrimination before the law
- Article 12 on privacy and protection of the law against attacks upon honour and reputation
- Article 19 on freedom of opinion and expression

Voluntary disclosure shall not be made to facilitate a prosecution that is political in nature or relates to the subject's race, religion, national origin, disability, sexual orientation, sex, marital status, gender identity or age.

It is also important that any direct request be justified under the necessity and proportionality principles, and that an SP does not breach any privacy or data protection obligations by producing BSI and/or traffic data in any applicable jurisdictions. When responding to direct requests, SPs must also comply with privacy obligations to users as defined in their privacy notice.

SPs can voluntarily research into States that do not apply due process or have alarming human rights records. Relevant resources would be the Department of State's Human Rights Reports or reports from Non-Governmental Organizations such as Human Rights Watch, Amnesty International, Access Now, Freedom House and Global Network Initiative.

There has been growing concern that SPs are increasingly being asked to act as regulators, quasi-judicial decision makers and human rights protectors. See chapter 6.1 for more information.

4.3 NON-EMERGENCY VOLUNTARY DISCLOSURE

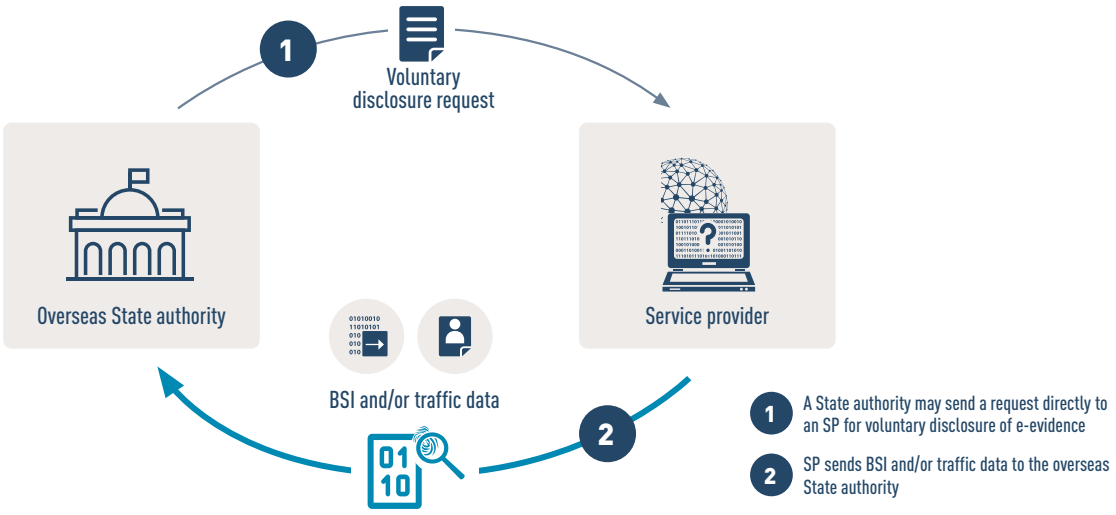
4.3.1 Receiving requests

It is very difficult to generalize operational practices on voluntary disclosure. For example, there is no explicit prohibition against direct contact in Canada or in the United States. Some United States SPs require a court order or legal proceeding for disclosure from the requesting State, and others have no procedure, on the basis that there is no legal requirement to disclose to a foreign request in United States law. Circumstances where a Canadian SP may disclose information without the consent of the data subject and without obtaining a court order or subpoena would be limited, and some SPs will, out of an abundance of caution, decline to provide information unless legally compelled to do so. It is important to note that SPs in these States are under no legal obligation to comply with an overseas direct request and any voluntary disclosure would need to comply with applicable privacy laws. SPs may wish to check all applicable laws for each case to determine the possibility of voluntary disclosure.

If voluntary disclosure is well conducted, this can greatly assist an investigation or prosecution and may mean that a requesting State does not need to send a mutual legal assistance request, saving resources and time for all parties concerned.

SPs may require an overseas State authority requesting voluntary disclosure to attach a copy of a domestic court order or legal process to ensure that the request has been independently reviewed and is lawfully justified.

[37] See also chapter 2.1.1 on United Nations and international legal standards.



Others evaluate the request on the basis of supporting information:

- Apple has a form.[38]
- Ebay has a law enforcement eRequest system with an online web-form designed for law enforcement to submit direct requests.[39]
- Direct requests to Facebook should be made through the law enforcement online request system and may require a domestic order.[40]
- Twitter may provide voluntary disclosure on a case-by-case basis where a domestic order has been issued in the requesting State – direct requests should be submitted through the Twitter legal request submissions site.[41]

If an SP does not have a specific template, a model form for overseas direct requests is provided in annex IV. This recommends that an overseas State authority satisfy the following standards in a direct request to a SP:

- Use valid identifiers, to allow the SP to easily locate the targeted user(s)/account(s).
- Make sure to specify which type of information and time period is required and their relevance to the offence.
- Narrow down the requested data to what is needed. Limit it to the specific product(s) or service(s) concerned. Do not make an overly broad request. This is the most common reason for refusal of requests for most SPs.
- Justify how the information requested will assist in the investigation.
- Check if a domestic order under national law is required according to SP law enforcement guidelines. Where law enforcement guidelines are not available it is good practice to apply for a domestic order and attach it to your request.
- Check confidentiality risks and attach to your request an order under domestic law and procedure for non-notification and non-disclosure at the same time as requesting the domestic order for the production of BSI and/or traffic data.
- Specify if an authentication statement of affidavit is required (if responses are not self-authenticating).

[38] www.apple.com/legal/privacy/gle-inforequest.pdf.
[39] https://lers.corp.ebay.com/.
[40] www.facebook.com/records
[41] https://legalrequests.twitter.com/forms/landing_disclaimer.

4.3.2 Model scenario

The model scenario of the New Country Counter-Terrorism Police below will assist with how a direct request is completed and submitted by overseas law enforcement to a SP.

Model scenario: The New Country Counter-Terrorism Police

After the comments posted by Victory4Mujahideen on the YouTube videos, the New Country Counter-Terrorism police require the BSI and traffic data from Google (YouTube) to determine the identity of Victory4Mujahideen and traffic data from Apple for email Akan007@icloud.com (the source and destination IP addresses of messages) to investigate who is part of the wider terrorist network. The New Country Counter-Terrorism police review the mapping in annex I and send a direct request to Google (YouTube) for voluntary disclosure of BSI and traffic data for Victory4Mujahideen using the Model Direct Request Form at annex IV (see completed form below).

DIRECT REQUEST FOR VOLUNTARY DISCLOSURE OF DATA
Date: 15 December 2020

REQUESTING AUTHORITY: New Country Counter-Terrorism Police
Identification details:
- Full name or personal identification number: Inspector Nicked (DI390)
- Position held: Inspector of Police

Contact details of authority's representative:
Phone number: +123(0)2435 627348 Ext: 553336
Email: di.nicked@police.nc

Proceedings number: n/a

ADDRESSEE (RECIPIENT): Google
Address: lis-global@google.com

This authority is conducting a criminal investigation (Operation Improve) that involves users from your platform. Electronic data has been deemed relevant in this matter. I am hereby requesting the disclosure of electronic data on a voluntary basis in relation to the user(s) and/or account(s) mentioned below.

Any and all information or data provided in response to this request will only be used in the described investigation and will not be disclosed to unauthorized personnel.

NATURE OF THE CASE:
Click here to describe the nature of the crime investigated. Provide as much information and context as possible, in relation to this particular request for electronic data.
Examples of information that may be provided here in addition to the nature of the case:
- *Status/progress (e.g., pre-arrest, pretrial, trial, crime in progress, ...)*
- *National criminal code article/law/statute defining the offence you are investigating*
- *Maximum sentence according to your national law*
- *Nationality or long-term residence if known*

The Internet Referral Unit (IRU) of the New Country Counter-Terrorism Police commenced the monitoring of a video on YouTube: Ground Zero: Syria (Part 7) - Snipers of Aleppo supporting the proscribed terrorist organization the Al-Nusrah Front. The IRU observed a comment posted by Victory4Mujahideen on 15 December 2020, stating, "Want to go for jihad Syria, email: Akan007@icloud.com" and "Allahu Akbar, I'm going as well insha'allah" Operation Improve has been commenced by the New Country Counter-Terrorism Police to determine the identity of Victory-4Mujahideen and user Akan007@icloud.com and investigate the offences of encouraging terrorism in New Country contrary to section 4 of the Anti-Terrorism Act 2007, dissemination of terrorist material contrary to section 2(3) of the Anti-Terrorism Act 2007 and membership of a proscribed terrorist organization (ANF) contrary to section 5 Terrorism Act 2007.

continued

LEGAL BASIS:
Lay down the legal basis under which the request is being made, according to domestic legislation.
Production of data relevant to a terrorism investigation pursuant to section 28 of the Anti-Terrorism Act 2007

DOMESTIC LEGAL PROCESS:
If required by the service provider, attach the domestic legal process for the requested data in accordance with legislation in your country.
See attached production order signed by Senior Magistrate Trombleau[a]

CONCERNED USER OR ACCOUNT:
Click here to enter all the information available about the subject of the investigation, (such as name, email address, account ID, phone number, device information, domain name for registry/registrar, Bitcoin address, Bitcoin transactions, IP addresses, credit card or bank account), to assist the company in identifying the accounts concerned.
If possible, state if the subject is a suspect, victim, witness or person of interest in your investigation.
It is also advised to include screenshots and full URLs, if available.

Victory4Mujahideen
See Screenshot of the message of 15 December 2020

INFORMATION REQUESTED:
This request applies to the items indicated below , whether in electronic or other form, including information stored on backup media, if available. A justification for the request for preservation of these data sets will follow.

Basic subscriber information for the user Victory4Mujahideen
- Full name provided
- Vanity name or login name
- User ID
- Phone number(s)
- Email address(es)
- Date of birth
- Billing information/means of payment
- Account start and end date
- Account status
- Registration IP address, including time stamp
- Associated devices (including IMEI, MAC address and UDID when available)
- Copy of ID card or passport provided by the subscriber
- Type of registration, copy of a contract, means of verification of identity at the moment of registration, copies of documents provided by the subscriber
- Any other information pertaining to the identity of the user/subscription holder

Traffic data for the user Victory4Mujahideen
- IP address logs, including time stamp
- Message logs and chat logs
- Activity log/logfiles, including time stamp
- Routing information (source IP address, destination IP address, port number, browser, email header, message ID, data transfer volume, source or destination of any electronic messages sent from or received from the account)

JUSTIFICATION, INCLUDING FOR NECESSITY AND PROPORTIONALITY:
Justify how the information to be preserved will assist in the investigation. If possible, make this justification for each specific piece of information requested above. Overbreadth is the most common reason companies give for refusal.

Operation Improve has commenced to determine the identity of account identifier Victory4Mujahideen after the user posted comments to an Al-Nusrah Front (ANF) video on YouTube: Ground Zero: Syria (Part 7) - Snipers of Aleppo on 15 December 2020: "Want to go for jihad Syria, email: Akan007@icloud.com" and "Allahu Akbar, I'm going as well insha'allah"

Al-Qaida is a proscribed terrorist organization in New Country pursuant to Schedule One of the Anti-Terrorism Act 2007. The ANF should be treated as alternative names for the organization which is already proscribed under the name Al-Qaida.

The basic subscriber information and traffic data will enable the New Country Counter-Terrorism Police to identify the user of account identifier Victory4Mujahideen and secure any evidence to support a prosecution for encouraging terrorism in New Country contrary to section 4 of the Anti-Terrorism Act 2007, dissemination of terrorist material contrary to section 2(3) of the Anti-Terrorism Act 2007 and membership of a proscribed terrorist organization (ANF) contrary to section 5 Terrorism Act 2007.

[a] For the purposes of this case scenario the production order is not attached but in practice the requester should apply for an order and then attach.

continued

TIME RANGE/PERIOD:
Specify here the time frame of the information to be preserved. Provide a time frame that is as narrow as possible to avoid making overly broad requests and specify the time zone.
Spell out the month, instead of using the number, as date format is different in the United States.
The requested time frame for the traffic data is from 14 December 2020 to the execution of this request. The 14 December 2020 is the day before the comment posted on 15 December 2020 by Victory4Mujahideen and will enable the New Country Counter-Terrorism Police to capture all traffic data for 15 December 2020.

CONFIDENTIALITY:
☒ I request that you do not disclose the existence of this request to the subscriber or any other person, other than as necessary to comply with this request. If compliance with this request might result in a permanent or temporary termination of service to the account(s), or otherwise alert any user of the account(s) as to your actions to disclose the information described below, please contact me as soon as possible before taking action

Click here to state the reasons why prohibition of notification to the user is requested. Specify the statute, if any, under which the non-disclosure request is being made. Please also include the end date of the user notice prohibition, if applicable.
If notice is prohibited to the subscriber, and you have obtained a domestic court order, attach it here.

As the identity of Victory4Mujahideen and Akan007@icloud.com are unknown, to notify the user of this preservation request would alert them and potentially other members of the terrorist organization Al-Qaida, of the nature and stage of the investigation. See attached non-notification and non-disclosure order pursuant to section 32 of the Anti-Terrorism Act 2007 signed by Senior Magistrate Trombleau.[b]

Attach court order if available

PGP: *Attach PGP Public Key (if applicable)*

SUMMARY OF DOCUMENTS ATTACHED:
1. Screenshot of comments by Victory4Mujahideen on 15 December 2020
2. Relevant law under the Anti-Terrorism Act 2007: Sections 2(3), 4, 5, 28 and 32 and Schedule One
3. Production order signed by Senior Magistrate Trombleau and dated 15 December 2020
4. Non-notification and non-disclosure order signed by Senior Magistrate Trombleau and dated 15 December 2020

If you have questions regarding this request, please contact me.

I hereby certify I have the legal authority to submit this request and that the information provided is true to the best of my knowledge.

Before submitting this request, print, sign and stamp it. Then, scan and submit it to the company digitally, following their guidelines.

NEW COUNTRY POLICE

Google voluntarily discloses that the YouTube account Victory4Mujahideen was opened with an email address of Akan007@icloud.com registered in the name A. Khan, date of birth 1980, address First District, Newtown, New Country. This address is associated to Amir Khan, who travelled to the Syrian Arab Republic with others to fight for the Al-Nusrah Front.

[b] For the purposes of this model scenario the production order is not attached but in practice the requester may attach such an order.

4.4.3 Non-emergency voluntary disclosure checklist

The following tables could be a useful voluntary disclosure request checklist.[42]

VOLUNTARY DISCLOSURE REQUEST CHECKLIST		
Date and time direct request received		
Who direct request is received from		
SENDER		
Who sent the request:		
Law enforcement officer	☐ Yes	☐ No
Is the officer's name included?	☐ Yes	☐ No
Is the officer's rank included?	☐ Yes	☐ No
Has the officer confirmed they have the required legal authority to make the request?	☐ Yes	☐ No
Has the request been sent from an official email address?	☐ Yes	☐ No
Has the request been authorized by a senior officer?	☐ Yes	☐ No
Prosecutor	☐ Yes	☐ No
Is the prosecutor's name included?	☐ Yes	☐ No
Has the prosecutor confirmed they have the required legal authority to make the request?	☐ Yes	☐ No
Has the request been sent from an official email address?	☐ Yes	☐ No
Judicial authority	☐ Yes	☐ No
Is the judge's name included?	☐ Yes	☐ No
Has the judge confirmed they have the required legal authority to make the request?	☐ Yes	☐ No
Has the request been sent from an official email address?	☐ Yes	☐ No

[42] Available in PDF format at: https://sherloc.unodc.org/cld/en/st/evidence/ddf.html

VOLUNTARY DISCLOSURE REQUEST CHECKLIST *(continued)*		
ACCOUNT IDENTIFIER		
Has the correct identifier been provided to enable the data to be preserved?	☐ Yes	☐ No
COURT ORDER OR JUDICIAL PROCESS		
Is a court order or judicial process from the requesting State attached?	☐ Yes	☐ No
DATA REQUESTED		
BSI?	☐ Yes	☐ No
Traffic data?	☐ Yes	☐ No
CRIMINAL INVESTIGATION		
Have the criminal offences been listed?	☐ Yes	☐ No
Has confirmation been provided that the data requested is linked to the investigation?	☐ Yes	☐ No
Is the data requested relevant to the investigation?	☐ Yes	☐ No
Is there a justifiable time frame for the requested data?	☐ Yes	☐ No
HUMAN RIGHTS		
Confirm request: Respects the right to life, liberty and security?	☐ Yes	☐ No
The request does not support an investigation where there has been or is likely to be torture or to cruel, inhuman or degrading treatment or punishment	☐ Yes	☐ No
The request does not support an investigation where there has been or is likely to be any discrimination to equal protection of the law	☐ Yes	☐ No
The request does not support an investigation where there has been or is likely to be any restriction of the right to freedom of opinion and expression	☐ Yes	☐ No

VOLUNTARY DISCLOSURE REQUEST CHECKLIST *(continued)*

HUMAN RIGHTS *(continued)*		
Voluntary disclosure is not made to facilitate a prosecution that is political in nature or relates to the subject's race, religion, national origin, disability, sexual orientation, sex, marital status, gender identity, age	☐ Yes	☐ No
Confirm sources checked to confirm the above.		
CONFIDENTIALITY		
Is a paragraph included not to notify the user of the existence of the request?	☐ Yes	☐ No
Confirm – even in absence of request – that the user will not be notified through termination of service	☐ Yes	☐ No
CONFIRMATION		
Has the sender been notified the request has been received?	☐ Yes	☐ No
Has the sender been notified when the data will be sent to them?	☐ Yes	☐ No
FURTHER REQUESTS		
Is the data self-authenticating?	☐ Yes	☐ No
Is there a request to provide the data in another format?	☐ Yes	☐ No
Can this be provided?	☐ Yes	☐ No
Confirm reasons why other formats cannot be provided (for example, data self-authenticating or will not agree for statement of affidavit to be used in trial proceedings)		

4.4 EMERGENCY VOLUNTARY DISCLOSURE

In emergency situations data can avert the risk of death or serious harm – this requires an efficient process to respond speedily to emergency disclosure requests.

In most cases, United States SPs can accept an emergency disclosure request for BSI and traffic data from an overseas State authority, particularly if the person making the request can establish they are genuinely a public official, such as by use of an email address from an official government domain and by providing official address and telephone contact details.

If an SP is not satisfied that a public official in a requesting State can establish their bona fides, it may be necessary to advise that their request be made via a recognized third party.

In the United States, legislation provides a procedure for the disclosure of data in emergency situations to United States law enforcement concerning domestic cases.

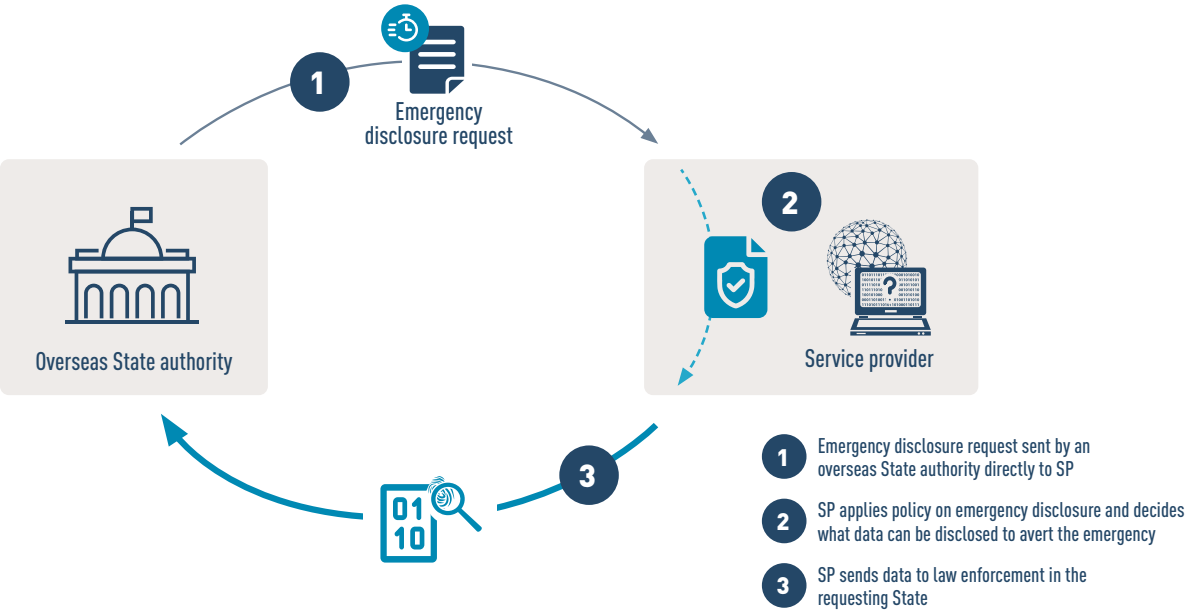
According to the ECPA § 2702(b)(8) or (c)(4),[43] an emergency is when there is:

- **An imminent danger of death or serious physical injury to any person** (Apple also includes circumstance(s) involving imminent and serious threat(s) to the security of a State and the security of critical infrastructure/installation(s)).
- **A need for requiring or justifying disclosure without delay.**

Although there is no legal requirement, many United States SPs apply the same legal provisions to respond to disclosure requests from overseas State authorities to prevent death or serious harm to individuals in emergency situations.

Case study: France

Following the Charlie Hebdo terrorist attack on 7 January 2015, the French authorities contacted the FBI, who made an emergency disclosure request to Microsoft for emails of two accounts. The request arrived electronically before 6 a.m. and Microsoft were able to review, extract the relevant data and send them to the FBI in 45 minutes for transmission to the French authorities.



[43] 18 US Code § 2702 - Voluntary disclosure of customer communications or records, (b)(8) and (c)(4).

4.4.1 Emergency v. urgency

"Imminence" is essential when determining if there is an actual emergency. The emergency request checklist in chapter 4.4.4 will assist SPs in determining if an emergency is imminent. If the imminence of death or serious physical injury can no longer be sustained, there will be no basis for SPs to disclose data.

It is important not to confuse "emergency situations" from general "urgent situations." Some emergency disclosure requests may request fast disclosure for following reasons:

However, such circumstances will not be regarded as an emergency if there is not an imminent danger of death or serious physical injury to any person, unless the SP sets additional grounds (in the case of Apple, for instance) for "security of a State and the security of critical infrastructure/installation(s)." There might be legal avenues such as MLA requests, seeking urgent action, but these should not be confused with an emergency.[44]

The following examples are commonly observed practices on determining emergency among United States SPs:

- Police have arrested a suspect and after accessing his mobile phone find an instant message referring to a distributed denial of service (DDoS) attack against an intensive care unit in a hospital ward with critically ill patients. The DDoS attack will prevent hospital staff from having access to essential data on patient files. Logfiles and the purchase history of the web hosting provider are needed to confirm who is behind the DDoS attack.
  Conclusion: This is an emergency due to the imminent danger of serious physical harm or death to the patients in intensive care if the DDoS attack takes place.
- Intelligence services have intercepted some communications from a terrorist group. It seems that a bombing attack could be imminent. To prevent the attack, there is need for source IP addresses from the instant messaging apps used by the terrorists.
  Conclusion: This is an emergency as there is an imminent danger of death or serious physical injury to people, although potential victims are unknown.
- A child was kidnapped and a threat was sent to her parents she would be killed if a ransom were not paid. The parents paid the ransom and the child was released. Those who carried out the kidnap have not been located.
  Conclusion: This is not an emergency as the danger of death or serious physical injury to the child is no longer imminent.
- A young girl has disappeared with no traces of violence. She has a Facebook account with some private information. Traffic data (source IP addresses) and content data could help police to locate her. Initially, an MLA request was issued with no success due to difficulties in meeting the probable cause for the content data. After some months, investigators tried with an emergency disclosure request directly to Facebook.
  Conclusion: This is not an emergency as the police could not prove the imminent danger of death or serious physical injury.

4.4.2 Information to be provided in an emergency request

Some SPs have their own emergency disclosure request form. For those SPs who do not have a form, see annex III for a model form for emergency disclosure requests.

Good practices on emergency disclosure requests may include the following:

- Account or user identifier, depending on the service and the specific policy of the SP.

[44] For the case of Canada, the Office of the Privacy Commissioner of Canada (OPC) said in their COVID-19 Guide that an emergency disclosure request would likely be permissible "if an individual requires urgent medical attention, and they are unable to communicate directly with medical professionals" and disclosure is necessary to safeguard the individual's health. See www.priv.gc.ca/en/privacy-topics/health-genetic-and-other-body-information/health-emergencies/gd_covid_202003/.

- Key details regarding the nature of the emergency and explanations on why the threat is credible. It is not enough to merely state that there is a bomb threat.
- The imminence of threatened death or serious physical injury. It can be helpful to provide key details, such as deadlines for receiving the requested information and the factual basis that supports the existence of the deadline.
- Explanations on how the data sought will assist in averting the threatened death or serious physical injury and that it cannot be obtained through any other methods.
- The type of data and time period required, and their relevance to the emergency.
- Narrowed down language on what is needed, limiting it to the specific product(s) or service(s) concerned. Avoid an overly broad request.
- All other available details or context regarding the particular circumstances.
- Identity of person (if known) who is in danger of death or serious physical injury.
- Identification of the specific data believed to be in the possession of the SP, and how it relates to the claimed emergency.
- A non-disclosure or gag order/request not to notify the user if such notification could exacerbate the emergency situation.
- A domestic order, if it is required under applicable law(s).

4.4.3 Model scenario

Model scenario: The New Country Counter-Terrorism Police

After Amir Khan is charged with terrorist offences in New Country, comments appear on a post on Baaz under the username VictoryStill4Mujahideen threatening to attack the New Town shopping mall on the day of his court appearance on the 17 December 2020 at 10 a.m.: "Jihad 17 December 2020 to New Town shopping mall or free AK Allahu Akbar, insha'allah". The New Country Counter-Terrorism Police submits an emergency dsclosure request below – using the model emergency disclosure request form from annex III.

Date: 17 December 2020

REQUESTING AUTHORITY: New Country Counter-Terrorism Police
Identification details:
- Full name or personal identification number: Inspector Nicked (DI390)
- Position held: Inspector of Police

Contact details of authority's representative:
Phone number: +123(0)2435 627348 Ext: 553336
Email: di.nicked@police.nc

Proceedings number: AmirKhan/15092021/1

ADDRESSEE (RECIPIENT): BAAZ
Address: info@baaz.com

This authority is conducting a criminal investigation that involves users from your platform. Electronic data has been deemed relevant in this matter. I am hereby submitting an emergency request for the disclosure of electronic data in relation to the user(s)/account(s) mentioned below.
VictoryStill4Mujahideen

continued

Any and all information or data provided in response to this request will only be used in the described investigation and will not be disclosed to unauthorized personnel.

NATURE OF THE EMERGENCY:
Click here to describe the imminent nature of the emergency. Provide as much information and context as possible, in relation to this particular request for electronic data.
Consider consulting each company specific criteria on emergency.
Examples of information that may be provided here in addition to the nature of the emergency:
- *Status/progress (e.g., pre-arrest, pretrial, trial, crime in progress, ...)*
- *National criminal code article/law/statute defining the offence you are investigating*
- *Maximum sentence according to your national law*
- *Nationality or long-term residence if known*

Amir Khan has been charged with terrorist offences in New Country related to fighting for the proscribed terrorist organization Al-Nusrah Front (ANF) in Syria. The investigation into his terrorist activities commenced after he posted comments with the username Victory4Mujahideen on a YouTube video supporting jihad in Syria with the ANF. A different username, VictoryStill4Mujahideen posted the following comments on a news report video on Baaz on 17 December 2020 at 07.12.47 CET confirming that Amir Khan had been charged and was due to appear in court on 17 December 2020: *"Jihad 17 December 2020 to New Town shopping mall or free AK Allahu Akbar, insha'allah"*.

Click here to describe the imminent nature of the threat or provide information that suggests there is a specific urgency to obtain the information from this service provider.
On the basis of the threat posted on the news report video on Baaz on 17 December 2020 at 07.12.47 CET about an imminent attack at the New Town Mall there is a good faith belief that there is an exigent emergency involving
- ✓ The danger of death or
- ✓ Serious physical injury to a person

LEGAL BASIS:
Lay down the legal basis under which the request is being made, according to domestic legislation.
An emergency disclosure request can be submitted to domestic service providers in terrorism cases pursuant to section 38 of the Anti-Terrorism Act 2007.

CONCERNED USER OR ACCOUNT:
Click here to enter all the information available about the subject of the investigation, (such as name, email address, account ID, phone number, device information, domain name for registry/registrar, Bitcoin address, Bitcoin transactions, IP addresses, credit card or bank account), to assist the company in identifying the concerned accounts.
If possible, state if the subject is a suspect, victim, witness or person of interest in your investigation.
It is also advised to include screenshots and full URLs, if available.

VictoryStill4Mujahideen
Screenshot attached of comments posted by VictoryStill4Mujahideenon on 17 December 2020 at 07.12.47 CET
PLEASE NOTE: The legal attaché has been contacted at the United States Embassy who can be contacted at legalattache@USembassy.org to confirm the information in this request.

INFORMATION REQUESTED TO AVERT THE EMERGENCY:
This request applies to the items indicated below, whether in electronic or other form, including information stored on backup media, if available. A justification for the request for disclosure of these data sets will follow.

Basic subscriber information
- Full name provided
- Vanity name or login name
- User ID
- Phone number(s)
- Email address(es)
- Date of birth
- Billing information/means of payment
- Account start and end date
- Account status
- Registration IP address, including time stamp
- Associated devices (including IMEI, MAC address and UDID when available)
- Copy of ID card or passport provided by the subscriber
- Type of registration, copy of a contract, means of verification of identity at the moment of registration, copies of documents provided by the subscriber
- Any other information pertaining to the identity of the user/subscription holder

continued

Traffic data

- IP address logs, including time stamp
- Message logs and chat logs
- Activity log/logfiles, including time stamp
- Routing information (source IP address, destination IP address, port number, browser, email header, message ID, data transfer volume, source or destination of any electronic messages sent from or received from the account)

JUSTIFICATION, INCLUDING FOR NECESSITY AND PROPORTIONALITY:
Justify how the information requested will assist in the investigation to avert the emergency and explain how the user, the account and each category of data sought is linked to the exigent circumstances. If possible, make this justification to each specific piece of information requested above. Overbreadth is the most common reason companies give for refusal.

The voluntary disclosure process and transmitting a Mutual Legal Assistance request are not appropriate in the circumstances to obtain the BSI and traffic data associated with VictoryStill4Mujahideen to prevent an imminent attack at the New Town shopping mall that will cause serious injury or kill individuals.

TIME RANGE/PERIOD:
Specify here the time frame of the information to be preserved. Provide a time frame that is as narrow as possible to avoid making overly broad requests and specify the time zone.
Spell out the month, instead of using the number, as date format is different in the United States.

PLEASE NOTE that the threat relates to an attack due to take place imminently at 10.00 hrs today and the BSI and traffic data is needed immediately to confirm the identity of the individual who is linked to the post at 07.12.47 CET – so the New Country Counter-Terrorism police can locate the individual concerned to prevent the attack.

CONFIDENTIALITY:
☒ *I request that you do not disclose the existence of this request to the subscriber or to any other person, other than as necessary to comply with this request. If compliance with this request might result in a permanent or temporary termination of service to the account(s), or otherwise alert any user of the account(s) as to your actions to disclose the information described below, please contact me as soon as possible before taking action*

Click here to state the reasons why prohibition of notification to the user is requested. Specify the statute, if any, under which the non-disclosure request is being made. Please also include the end date of the user notice prohibition, if applicable.
If notice is prohibited to the subscriber, and you have obtained a domestic court order attach here.

This is a covert investigation and to alert the user VictoryStill4Mujahideen could hamper the investigation to avert the emergency, resulting in injury or death to citizens present in the New Town shopping mall.

Attach court order if available

PGP: *Attach PGP Public Key (if applicable)*

SUMMARY OF DOCUMENTS ATTACHED:

Screenshot attached of comments posted by VictoryStill4Mujahideenon on 17 December 2021 at 07.12.47 CET

If you have questions regarding this request, please contact me.

I hereby certify I have the legal authority to submit this request and that the information provided is true to the best of my knowledge.

Before submitting this request, print, sign and stamp it. Then, scan and submit it to the company digitally, following their guidelines.

NEW COUNTRY POLICE

4.4.4 Voluntary disclosure checklists for emergency and non-emergency

The following tables could be a useful emergency voluntary disclosure request checklist.[45]

EMERGENCY DISCLOSURE REQUEST CHECKLIST		
Date and time emergency request received		
Who emergency request is received from		
SENDER		
Who sent the request:		
Law enforcement officer	☐ Yes	☐ No
Is the officer's name included?	☐ Yes	☐ No
Is the officer's rank included?	☐ Yes	☐ No
Has the officer confirmed they have the required legal authority to make the request?	☐ Yes	☐ No
Has the request been sent from an official email address?	☐ Yes	☐ No
Has the request been authorized by a senior officer?	☐ Yes	☐ No
Prosecutor	☐ Yes	☐ No
Is the prosecutor's name included?	☐ Yes	☐ No
Has the prosecutor confirmed they have the required legal authority to make the request?	☐ Yes	☐ No
Has the request been sent from an official email address?	☐ Yes	☐ No
Judicial authority	☐ Yes	☐ No
Is the judge's name included?	☐ Yes	☐ No
Has the judge confirmed they have the required legal authority to make the request?	☐ Yes	☐ No
Has the request been sent from an official email address?	☐ Yes	☐ No

[45] Available in PDF format at: https://sherloc.unodc.org/cld/en/st/evidence/ddf.html

EMERGENCY DISCLOSURE REQUEST CHECKLIST *(continued)*

ACCOUNT IDENTIFIER

Has the correct identifier been provided to enable the data to be preserved?	☐ Yes	☐ No

DATA REQUESTED

BSI?	☐ Yes	☐ No
Traffic?	☐ Yes	☐ No

EMERGENCY

Has a description been included of the emergency?	☐ Yes	☐ No
Is there a risk of death?	☐ Yes	☐ No
Or is there a risk of serious physical injury to a person?	☐ Yes	☐ No
Is the risk of death or of serious physical injury imminent? For example:	☐ Yes	☐ No

- An event that is about to happen or immediately threatened – for example, a terrorist attack
- An immediate threat to the safety of a child
- An event that is about to happen or immediately threatened to critical infrastructure[a] – for example, a distributed denial-of-service (DDoS) attack that would prevent air traffic control of airplanes
- An event that is about to happen or immediately threatened to the capability of institutions to protect individuals from serious physical harm or death – for example, hospitals

LINK TO EMERGENCY

Has confirmation been provided as to how the data requested is linked to the emergency?	☐ Yes	☐ No
Will data requested avert the risk of death and or serious physical harm to a person?	☐ Yes	☐ No

PROPORTIONALITY

Is there an explanation why the data cannot be obtained through other legal measures to avert the emergency?	☐ Yes	☐ No
Can the data only be obtained to prevent the emergency through an emergency disclosure request?	☐ Yes	☐ No

[a] For emergency disclosure requests to SPs in the United States, see the Department of Homeland Security list of 16 critical infrastructure sectors at: www.dhs.gov/critical-infrastructure-sectors

EMERGENCY DISCLOSURE REQUEST CHECKLIST *(continued)*		
CONFIDENTIALITY		
Is a paragraph included not to notify the user of the existence of the request?	☐ Yes	☐ No
Confirm – even in absence of request – that the user will not be notified through termination of service	☐ Yes	☐ No
OTHER INFORMATION		
For a United States EDR, has the FBI attaché at the local United States Embassy verified the emergency?	☐ Yes	☐ No
CONFIRMATION		
Has the sender been notified the request has been received?	☐ Yes	☐ No
Has the sender been notified when the data will be sent to them?	☐ Yes	☐ No

CHAPTER 5.
MUTUAL LEGAL ASSISTANCE

5.1 BASIC CONCEPTS

Mutual legal assistance (MLA) refers to the support that Member States provide to each other during investigations, prosecutions and judicial proceedings in criminal, civil or administrative matters. MLA is generally used for seeking material that cannot be obtained on a police cooperation basis, particularly enquiries that require coercive means. This assistance is usually requested by courts or prosecutors and is also referred to as "judicial cooperation".

MLA is a formal government-to-government type of assistance that can be based on:

- An international or bilateral treaty or agreement
- Applicable domestic legislation
- The principle of reciprocity

MLA can be requested for purposes such as:

- Gathering evidence, including electronic
- Taking evidence or statements from persons
- The service of judicial documents
- Executing searches and seizures
- Providing information, evidentiary items and expert evaluations
- The transfer of sentenced persons

MLA can be requested for any type of assistance, if it is not contrary to the law of the States involved.

Most countries have designated a central authority for MLA, often in response to obligations contained in treaties they are parties to, such as the United Nations Convention against Transnational Organized Crime. The central authority may be department(s) (often devoted to international legal assistance) within the General Prosecutors' Offices, Ministry of Justice or Ministry of Foreign Affairs. While these are among the most observed types of central authority, each State is free to decide the modality of its own central authority. The contact details of central authorities are available to all government officials within the password protected UNODC Online Directory of Competent National Authorities.

Once a State has identified the need to initiate an MLA process, it will start by sending a formal international letter of request known as a mutual legal assistance request. Central authorities are normally the focal points for receiving and sending MLA requests. In most cases, an MLA request is sent by the requesting State's central authority to the requested State's central authority, unless otherwise indicated. In some cases, depending on the request, it can be channelled through the National Central Bureau of INTERPOL.

Once an MLA request is received, the requested State's central authority may, if it has the power to do so, execute the request. If, as may be the case in many States, the central authority does not have the power to execute an incoming MLA request, it must then transmit it to other competent authorities within their jurisdiction. These may include, depending on the jurisdiction, the following:

- Law enforcement
- Police or investigative agencies
- Judiciary
- Ministries of Interior/Home Affairs
- National or Supreme Courts
- General Prosecutor's Offices
- Financial intelligence units
- Penitentiary departments, etc.

Determining which competent authorities will be engaged in executing an MLA request depends on the way each State has organized its own internal system as well as on the type of assistance sought in the MLA request itself.

Practical note:

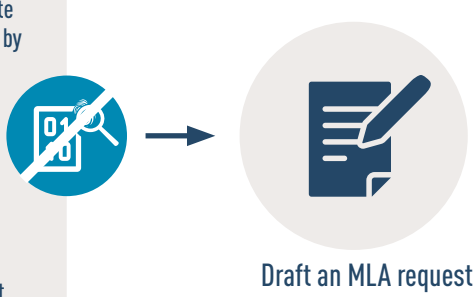
Mutual legal assistance shall be afforded under relevant laws, treaties, agreements and arrangements of the requested State.

The following resources are published for criminal justice officials but may also assist SPs in understanding the concepts.

- Revised Manuals on the Model Treaty on Extradition and on the Model Treaty on Mutual Assistance in Criminal Matters
- Model Law on Mutual Legal Assistance in Criminal Matters, 2007
- Model Treaty on Mutual Assistance in Criminal Matters, 1998
- Model MLA request for stored BSI, traffic data or content data
- Model MLA request for real-time collection of e-evidence
- Checklist for the drafting of an MLA request for e-evidence and essential steps

If admissible e-evidence cannot be obtained through non-MLA mechanisms because:

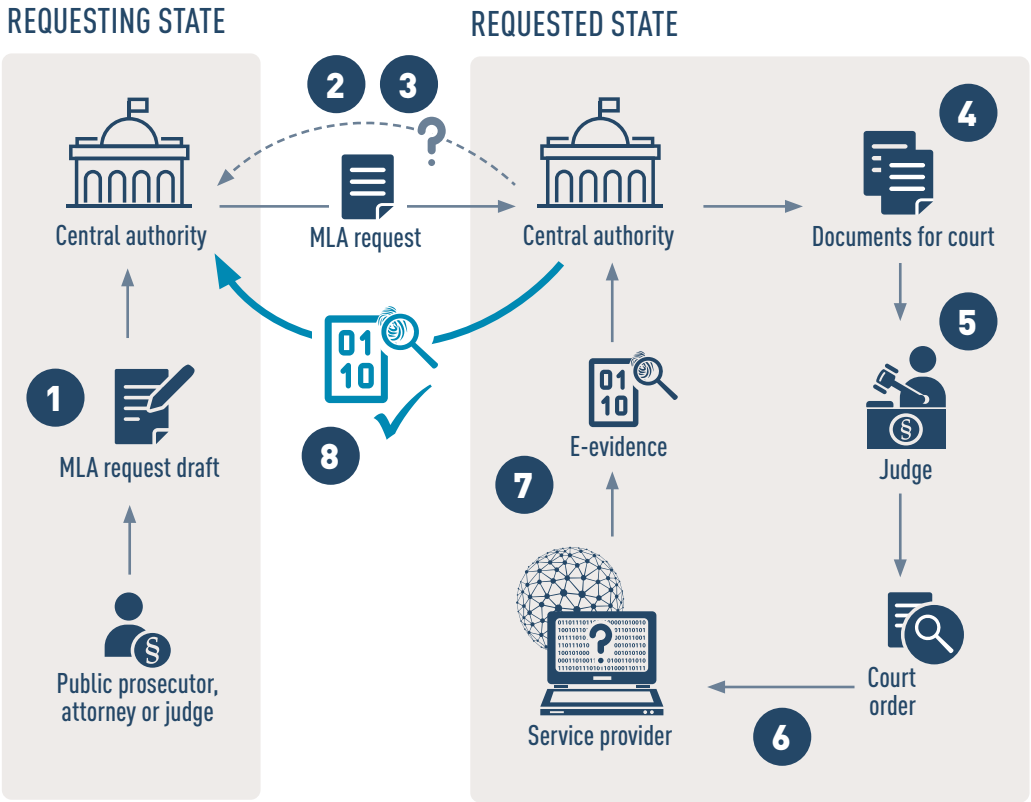
- The data is unavailable through open-source searches.
- SPs do not disclose e-evidence in voluntary response to overseas State authorities (i.e., voluntary disclosure), or such an action is prohibited by relevant law.
  The prohibition might not be in the local jurisdiction in which the company is based, but other laws might apply. For example, for a hosting or multilayered service provider, the law in the country in which the direct platform customer is located if the request is coming from a third country (e.g., where an end user or consumer is located. See 6.4 Hosting or multilayered providers).
- The data cannot be preserved and must be obtained quickly to prevent deletion;
- E-evidence obtained by voluntary disclosure is inadequate to satisfy the requesting State's requirements for admissibility at trial.



A mutual legal assistance request will be sent by the requesting State to the jurisdiction where the SP operates for a court order to compel the production of e-evidence.

5.2 GENERAL PRACTICES

While practices may vary depending on the jurisdiction, this chapter shows a possible MLA workflow to introduce basic concepts.



5.2.1 Requesting data

In order to obtain data stored in foreign jurisdiction, the requesting State may spell out in its MLA request how the data sought is relevant and related to a criminal investigation. It is not enough to show that the suspect or accused had an email account or social media account; the account must have something to do with the crime being investigated. For example, the BSI of a phishing email is required by law enforcement to try and identify the sender.

In many jurisdictions, MLA requests involving the disclosure of content data require higher standards of necessity and proportionality than other requests for non-content data. This will depend on the data protection legal framework in force in each jurisdiction.

SPs may wish to note that an MLA request can be refused if, in the view of the requested State, it would cause risks related to the protection of fundamental human rights.

5.2.2 Data production

If an SP is served with a copy of a legal order to produce e-evidence, the SP should locate and produce the requested data as soon as practicable. If the requested data has been preserved by the SP, which is often the case, they are likely to be able to respond to the legal request quickly.

The legal order may include a request that any produced data be certified by the SP in a manner that would make them admissible in future court

proceedings in the requested State. The declaration of the SP is requested at times, and this may only be an indication that the legal order is requested by another State. A pro forma from the requested State may be attached to the legal order for the SP to complete. Or the SP may be required to provide a custodian of records declaration to verify the authenticity of the data produced after service of the legal request.

Depending on the jurisdiction, the legal order may specify the format used by the SP to produce the requested data. On many occasions, this should be in a format readable by the requesting State, so it can be used at trial.

5.2.3 Non-disclosure and sealing

While the term may vary in different jurisdictions, a non-disclosure or gag order may also be attached to the legal order, preventing the SP notifying the user. Any legal order may also be kept confidential using a sealing order, meaning all court filings (including the MLA request) pertaining to the matter would not be accessible to the public for a fixed time.

CHAPTER 6.
TRENDS AND CHALLENGES

6.1 QUASI-JUDICIAL ROLE OF SPs

The exponential growth of hosting of user data online by SPs has correspondingly led to important policy debates at the international, regional and domestic level on the role of States and SPs in handling access to data. Practitioners of e-evidence navigate an ever-changing legal environment to bring criminals to justice, fight against impunity and offer remedies to victims of crime.

The human rights obligations of States, including online, are clearly laid out in the Practical Guide. At the same time, however, businesses should support and respect the protection of internationally proclaimed human rights (Principle 1), as well as make sure that they are not complicit in human rights abuses (Principle 2),[46] [47] as enshrined in the principles of the United Nations Global Compact.

The Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism has expressed concerns that, in the context of the Global Initiative, large Internet SPs are increasingly asked to act as regulators, quasi-judicial decision makers and human rights protectors, roles they are ill-suited to take on.[48] First, SPs are given significant autonomy to set their policies on data retention, user notification of data preservation or collection requests, and on which State law enforcement entities they will voluntarily comply with. The Special Rapporteur has raised concerns about this role in other contexts and deemed it inconsistent with best human rights standards.[49] The Special Rapporteur considers that as SPs each establish their own procedure taking into consideration applicable laws, human rights norms and the particularities of their services and products, the integration of human rights law into SP policies and their capacity to evaluate the proportionality and necessity of the data requested, vary significantly and is generally insufficiently transparent.

For many human rights defenders, the more fundamental issue is that the SPs are being asked to play a quasi-judicial role.[50] The Special Rapporteur considered that States should not expect SPs to be sufficiently equipped and knowledgeable to assess the impact of a data request on the fundamental rights of an affected person, nor do they have a meaningful incentive to do so.[51] That obligation remains with the State and should be positively affirmed.

6.2 JURISDICTION AND THE CLOUD

6.2.1 Legal challenges

Data in the Cloud may be in permanent migration, meaning different parts of data can be located in different States at the same time. At the same time, national legislation often refers to the traditional concept of the territory of a State and not extraterritoriality. The services offered by a foreign SP may be available in a State, but this does not necessarily mean that national legislation can require the SP (located in another State) to disclose the data. Even if there is a branch office of the SP in the territory, it is possible that the office has no decision-making power on data disclosure. This can create difficulties for State authorities in knowing where requests[52] for e-evidence should be sent.

As described in chapter 2.2, this document recommends e-evidence requests be sent to the

[46] www.unglobalcompact.org/what-is-gc/mission/principles
[47] Also see Global Network Initiative (GNI) Principles as a voluntary commitment example.
[48] Input dated November 30, 2020.
[49] www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23494&
[50] See the Internet & Jurisdiction Policy Network's Global Status Report 2019 pp.65-69 www.internetjurisdiction.net/uploads/pdfs/GSR2019/Internet-Jurisdiction-Global-Status-Report-2019_web.pdf
[51] EDRi, *Position Paper on Cross-Border Access to Data*, p.16.
[52] This includes preservation requests, direct requests for voluntary disclosure, emergency disclosure requests and MLA requests.

establishment or legal representation of the SP that is responsible for data disclosure. However, in general, the legal relations between the territory and data still remain uncertain in many jurisdictions.

A number of States have begun to explore under what conditions authorities may request access to data using their own domestic tools. The Yahoo![53] decision in Belgium is an example of a recent court case which focuses on the legitimacy of the use of domestic production orders for companies whose main seat is outside the requesting State, but provide a service in the territory of that State. The resulting fragmentation may generate legal uncertainty, delays, as well as concerns for the protection of fundamental rights and procedural safeguards for persons related to such requests.[54]

Case study: Belgium

Skype Belgium: see Court of Cassation, case nr. P.17.1229.N, 19 February 2019 from page 6 of the Eurojust Cybercrime Judicial Monitor. In this case a Belgian investigating magistrate ordered the interception of communications through Skype which was located in Luxembourg. Skype refused to comply with the request on the basis that it was not sent through mutual legal assistance channels. The Supreme Court in Belgium reasoned that the Code of Criminal Procedure allowed the Belgian investigating magistrate, to make the order as the communications were conducted in Belgium, regardless of the location of that operator or provider. The Supreme Court held that the cooperation did not require intervention by the Belgian judicial authorities abroad, meaning there was no need for a request for mutual legal assistance to Luxembourg, where the provider has its establishment or infrastructure.

6.2.2 Law reform

Second Additional Protocol to the Budapest Convention on Cybercrime

In June 2017, the Cybercrime Convention Committee agreed on the terms of reference for the preparation of a second Additional Protocol to the Budapest Convention on Cybercrime and negotiations commenced in September 2017. The following elements, among others, are to be considered: *(a)* procedures enhancing direct cooperation with providers and entities in other Parties; *(b)* procedures enhancing international cooperation between authorities for the disclosure of stored computer data; *(c)* procedures pertaining to emergency mutual legal assistance; *(d)* procedures pertaining to international cooperation in the absence of applicable international agreements. The final provisional text of the Protocol was approved by the Cybercrime Convention Committee in May 2021 and its formal adoption is expected in November 2021.[55] [56]

[53] Belgium Yahoo! Case 3 Hof van Cassatie of Belgium, YAHOO! Inc., No. P.13.2082.N of 1 December 2015. See Eurojust's Cybercrime Judicial Monitor No 1 (pp.13-31): www.eurojust.europa.eu/sites/default/files/Publications/Reports/2016-06_CJM-1_EN.pdf

[54] Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, page 5.

[55] More information on the negotiations, approval of the draft "2nd Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence" and the final provisional text.

[56] In States Parties of the Convention on Cybercrime, under article 19 (2), a law enforcement authority may extend their search to data in the Cloud where it is accessible from a computer system on their territory and they have grounds to believe, that data is stored in another computer system on the same territory.

CLOUD Act

On 23 March 2018, the CLOUD Act (Clarifying Lawful Overseas Use of Data Act) became law in the United States in order to address some of the current challenges faced by law enforcement with respect to e-evidence.[57] It clarified that United States warrants require SPs to produce data in their possession, custody or control, regardless of whether they choose to store the data inside or outside the United States.

The CLOUD Act also authorizes the Government to enter into executive agreements under which the United States and its partner States may commit to removing legal impediments to cross-border compliance with legal orders in cases that involve serious crimes including terrorism. Only States with robust laws protecting privacy and civil liberties are eligible for such agreements. The framework is a supplement and not a replacement for the cooperation available through MLA.

The United Kingdom became the first State to enter into CLOUD Act Executive Agreement with the United States on 3 October 2019. This Agreement permits each State to send domestic legal requests directly to foreign SPs in the other State, but has yet to enter into force.

European Union e-evidence regulation and directive proposal

On 17 April 2018, the European Commission proposed new rules[58] to make it easier and faster for State authorities to obtain e-evidence from the Cloud through the following:

- *European Preservation Order:* This will allow a judicial authority in one Member State to oblige an SP offering services in the European Union and established or represented in another Member State to preserve specific data to enable the authority to request this information later via MLA, a European Investigation Order or a European Production Order.
- *European Production Order:* This will allow a judicial authority in one Member State to request e-evidence directly from an SP offering services in the European Union and established or represented in another Member State, regardless of the location of the data, which will be obliged to respond within 10 days, and within 6 hours in cases of emergency.

The open-ended ad hoc intergovernmental committee of the United Nations

In December 2019, the General Assembly approved a proposal entitled "Countering the use of information and communications technologies for criminal purposes" that aims to establish an open-ended ad hoc intergovernmental committee of experts, representative of all regions, to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes.[59]

[57] See more information on the CLOUD Act here: www.justice.gov/dag/cloudact.

[58] European Commission: proposal on e-evidence, with a regulation and a directive; Council of the European Union: Press release and the Council's general approach on the directive on harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings
European Parliament: status brief and the first/single reading

[59] A/RES/74/247: https://undocs.org/en/A/RES/74/247
See also: www.unodc.org/unodc/en/cybercrime/cybercrime-adhoc-committee.html

6.3 TRANSBORDER DATA FLOWS

The regulation of transborder data flows is currently gaining a considerable degree of attention, and much is unsettled. In particular, the regulation of data flow between the European Union and the United States has been in focus since the July 16, 2020 decision[60] in which the Court of Justice of the European Union invalidated the European Union–United States Privacy Shield that previously facilitated data flow between the European Union and the United States. However, the regulation of transborder data flows is clearly a global issue and not limited to the European Union–United States context. Furthermore, it is an issue connected to hotly debated topics such as "data sovereignty"[61] and "data localization"[62] which add to the complexity. Particularly calls for data localization have been justified by the need to facilitate law enforcement access to e-evidence. The efficiency of such an approach is, however, still being debated.

6.4 HOSTING OR MULTILAYERED PROVIDERS

Certain SPs may host other companies rather than having direct interactions with end users – meaning that they provide services or tools to an individual or entity who uses the services of the SP to contact or engage with an independent end user. This type of service design is not only limited to domain names registries and registrars. Some SPs have direct interaction with both client companies and end users, while some interact mostly with their client companies. These types of situations can present challenges, because beyond the laws of the jurisdiction of the SP and the end user, the SP may be constrained by the laws of the entity using its services directly.

For example, an SP located in Canada may provide services to an entity based in Europe. That European entity may use the tools of the SP to contact and harm an individual in the United States. A United States State authority would be likely to have a legitimate interest in protecting their resident and may seek information from the SP. However, in that circumstance the contact an SP may have with the United States may only be incidental, and limited to disclosing information subject to the laws of the jurisdiction of its direct customer (in this case, Europe). These types of multilayered relationships can create complicated and often overlapping sets of obligations and requirements, and can generate unexpected obstacles that might prevent an SP from otherwise disclosing relevant information.

[60] Case C-311/18 *Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems*.

[61] See for example, Internet & Jurisdiction Policy Network, *We Need to Talk About Data: Framing the Debate Around the Free Flow of Data and Data Sovereignty*, www.internetjurisdiction.net/news/aboutdata-report.

[62] See for example, Svantesson, D. *Data localisation trends and challenges: Considerations for the review of the Privacy Guidelines*, OECD Digital Economy Papers, No. 301. http://dx.doi.org/10.1787/7fbaed62-en

ANNEXES

I. Sample law enforcement guidelines
II. Model preservation request form
III. Model emergency disclosure request form
IV. Model direct request form for voluntary disclosure
V. Data retention laws for selected States

ANNEX I. SAMPLE LAW ENFORCEMENT GUIDELINES

The following sample law enforcement guidelines may assist SPs without their own guidelines to explore other practices.

Adobe
www.adobe.com/legal/lawenforcementrequests/law-enforcement.html (for North America)

www.adobe.com/legal/lawenforcementrequests/law-enforcement-intl.html (Outside of North America)

Airbnb
www.airbnb.com/help/article/960/how-does-airbnb-respond-to-data-requests-from-law-enforcement#procedures-for-non-us-law-enforcement-requests

AliExpress
https://alibabagroup.com/en/contact/law_e_commerce

Alibaba
https://alibabagroup.com/en/contact/law_e_commerce

Amino
https://support.aminoapps.com/hc/en-us/sections/115000567033-Resources-for-Law-Enforcement

Aol
www.eff.org/document/aol-law-enforcement-guide

Apple
www.apple.com/legal/privacy/law-enforcement-guidelines-outside-us.pdf (Outside of the United States)

www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf (US)

Ask.fm
https://safety.ask.fm/ask-fm-guide-for-law-enforcement-requests/

Atlassian
www.atlassian.com/trust/privacy/guidelines-for-law-enforcement

Badoo
https://badoo.com/en/team/contacts

Booking.com
www.booking.com/content/law-enforcement.en-gb.html

Blacknight
www.blacknight.com/legal/law-enforcement-guidelines/

Box
www.box.com/legal/law-enforcement-guidelines

Ebay
https://ir.ebaystatic.com/cr/v/c1/security_center/docs/eBay_LE_Guide_NA_2018_STACI.pdf

Facebook
www.facebook.com/safety/groups/law/guidelines

GitHub
https://help.github.com/en/github/site-policy/guidelines-for-legal-requests-of-user-data

Gmail
https://support.google.com/transparencyreport/answer/7381738?hl=en

GoFundMe
www.gofundme.com/legal

Google
https://policies.google.com/terms/information-requests?hl=en-US

Instagram
https://help.instagram.com/494561080557017

Ionos
www.ionos.com/help/my-account/legal-accordian/copyright-infringement/what-is-11-ionoss-subpoena-and-copyright-policy/

Kik
https://medialabai.force.com/KikHelpCenter/s/topiccatalog/law-enforcement

Line
https://linecorp.com/en/security/article/291
https://linecorp.com/en/security/article/35

LinkedIn
www.linkedin.com/help/linkedin/answer/56372

Mega
https://mega.nz/takedown

Mail.com
www.mail.com/company/subpoena/

Namecheap
www.namecheap.com/legal/general/court-order-and-subpoena-policy/

PayPal
https://safetyhub.paypal.com

ProtonMail
https://protonmail.com/law-enforcement

Pinterest
https://help.pinterest.com/en/article/law-enforcement-guidelines

Reddit
www.redditinc.com/policies/guideline-for-law-enforcement

Rocket.Chat
https://docs.rocket.chat/legal/guidelines-for-law-enforcement

Shopify
www.shopify.com/legal/gvtaccesspolicy

Snapchat
www.snapchat.com/lawenforcement

Surespot
www.surespot.me/documents/surespot_law_enforcement_guidelines.html

SoundCloud
https://soundcloud.com/law-enforcement-guidelines

TikTok
www.tiktok.com/legal/law-enforcement?lang=en

Twitter
https://help.twitter.com/en/rules-and-policies/twitter-law-enforcement-support

TextNow
https://help.textnow.com/hc/en-us/sections/360007311953-Law-Enforcement-Information

Tumblr
www.tumblr.com/docs/en/legal_guidelines

Twitch
www.twitch.tv/p/en/legal/terms-of-service/#17-requests-for-information-and-how-to-serve-a-subpoena

Uber
www.uber.com/legal/en/document/?name=guidelines-for-law-enforcement&country=united-states&lang=en (US)
www.uber.com/legal/en/document/?name=guidelines-for-law-enforcement&country=netherlands&lang=en-gb (Outside the US)

Vimeo
https://vimeo.com/leo/guidelines

VK(Vkontakte/ВКонтакте)
https://vk.com/data_protection?section=requests&lang=en (Only for Russian Law Enforcement authorities)

WhatsApp
https://faq.whatsapp.com/en/android/26000050/?category=5245250

Wechat
www.wechat.com/en/law_enforcement_data_request.html

Wish
www.wish.com/law-enforcement-policy

Wickr
wickr.com/privacy/#legalprocess

WordPress.com
https://en.support.wordpress.com/report-blogs/legal-guidelines/

YouTube
https://support.google.com/transparencyreport/answer/7381738?hl=en

Zoom
https://zoom.us/docs/en-us/government-requests-guide.html

ANNEX II. MODEL PRESERVATION REQUEST FORM

The forms, as included in this publication, are for reference and training purposes. In order to make edits to these forms, practitioners must download the forms' interactive version from the UNODC Sherloc Electronic Evidence Hub: https://sherloc.unodc.org/cld/en/st/evidence/model-forms.html.

INSERT LETTERHEAD OF THE REQUESTING AUTHORITY HERE

REQUEST FOR THE PRESERVATION OF ELECTRONIC DATA

Date

REQUESTING AUTHORITY:

Identification details

Full name or personal identification number

Position held

Contact details of authority's representative

Official email address and phone number

Proceedings number

Case number **Previous request numbers**

ADDRESSEE (RECIPIENT):

Address

This authority is conducting a criminal investigation that involves users from your platform. Electronic data has been deemed relevant in this matter. I am hereby requesting your company to immediately take all necessary actions to preserve and safeguard electronic data in relation to the below mentioned user(s) and/or account(s).

TYPE OF PRESERVATION REQUEST:

- New preservation request
- Request for extension of preservation period. If so, inform:

  Reference number of previous request(s) as provided by the company, if available:

  Date of submission of previous preservation request:

  Date of expiration of previous preservation request:

  Reason to request extension of preservation period:

REQUEST FOR THE PRESERVATION OF ELECTRONIC DATA 1

This model form is provided by UNODC, UN CTED, Europol, Eurojust and Cepol (via the projects SIRIUS, Euromed Justice and Euromed Police). These institutions have not reviewed and are not responsible for the content of this request.
You are responsible for complying with the relevant laws and procedure regarding data categorization and privacy when making and processing any request.

NATURE OF THE CASE:

Attach file

LEGAL BASIS:

DOMESTIC LEGAL PROCESS:

If required by the service provider, attach the domestic legal process for the requested information to be preserved in accordance with legislation in your country.

Delete file

Attach file

CONCERNED USER(S) OR ACCOUNT(S):

Delete file

Attach file

DATASETS:

This request applies to the items indicated below, whether in electronic or other form, including information stored on backup media, if available. A justification for the request for preservation of these datasets will follow.

Basic subscriber information

- ☐ Full name provided
- ☐ Vanity name, nickname or login name
- ☐ User ID
- ☐ Phone number(s)
- ☐ Email address(es)
- ☐ Date of birth
- ☐ Billing information/means of payment
- ☐ Account start and end date
- ☐ Account status
- ☐ Registration IP address, including time stamp
- ☐ Associated devices (including device ID, IMEI, MAC address and UDID when available)
- ☐ Copy of ID card or passport provided by the subscriber
- ☐ Type of registration, copy of a contract, means of verification of identity at the moment of registration, copies of documents provided by the subscriber
- ☐ Any other information pertaining to the identity of the user/subscription holder

For registries and registrars:

- ☐ Registrant, technical and administrative name, address, phone, fax number and email address of the specified domain
- ☐ Creation, updated date, current status and name servers of the specified domain

Other information:

Traffic data

- ☐ IP address logs, including time stamp
- ☐ Message logs and chat logs
- ☐ Activity log/logfiles, including time stamp
- ☐ Routing information (source IP address, destination IP address, port number, browser, email header, message ID, data transfer volume, source or destination of any electronic messages sent from or received from the account)
- ☐ Cryptocurrency address(es)

Other information:

Content data

- ☐ Contacts
- ☐ Messages
- ☐ Posts
- ☐ Media files: videos, photos, documents

- ☐ Mailbox dump
- ☐ Device backup
- ☐ Geolocation data, including time stamp
- ☐ Deposit/withdrawal/transaction history
- ☐ Account balance
- ☐ Profile photo(s)

Other information:

Other data

JUSTIFICATION, INCLUDING FOR NECESSITY AND PROPORTIONALITY:

TIME RANGE/PERIOD:

FOLLOW UP:

- ☐ Direct request for the disclosure of electronic data on a voluntary basis.
- ☐ Formal judicial request for the disclosure of electronic data under international judicial cooperation.

CONFIDENTIALITY:

☐ I request that you do not disclose the existence of this request to the subscriber or any other person, other than as necessary to comply with this request. If compliance with this request might result in a permanent or temporary termination of service to the account(s), or otherwise alert any user of the account(s) as to your actions to disclose the information described above, please contact me as soon as possible before taking action.

Attach court order if available

Attach file

PGP:

Attach PGP public key (if applicable)

Attach file

SUMMARY OF DOCUMENTS ATTACHED:

Open attachments pane

If you have questions regarding this request, please contact me.

I hereby certify I have the legal authority to submit this request and that the information provided is true to the best of my knowledge.

Insert stamp

Delete stamp

Insert signature

Delete signature

SIGN ELECTRONICALLY (once electronically signed the request cannot be edited)

Insert digital signature

Insert signature and stamp as images, sign the document electronically or print, stamp and sign it using a blue or black pen.

Best practices

Save editable

Print

Finalize

ANNEX III. MODEL EMERGENCY DISCLOSURE REQUEST FORM

The forms, as included in this publication, are for reference and training purposes. In order to make edits to these forms, practitioners must download the forms' interactive version from the UNODC Sherloc Electronic Evidence Hub: https://sherloc.unodc.org/cld/en/st/evidence/model-forms.html.

INSERT LETTERHEAD OF THE REQUESTING AUTHORITY HERE

EMERGENCY DISCLOSURE REQUEST

Date

REQUESTING AUTHORITY:

Identification details

Full name or personal identification number

Position held

Contact details of authority's representative

Official email address and phone number

Proceedings number

Case number **Previous request numbers**

ADDRESSEE (RECIPIENT):

Address

This authority is conducting a criminal investigation that involves users from your platform. Electronic data has been deemed relevant in this matter. I am hereby submitting an emergency request for the disclosure of electronic data in relation to the below mentioned user(s)/account(s).

Any and all information or data provided in response to this request will only be used in the described investigation and will not be disclosed to unauthorized personnel.

NATURE OF THE EMERGENCY:

Attach file

EMERGENCY DISCLOSURE REQUEST 1

This model form is provided by UNODC, UN CTED, Europol, Eurojust and Cepol (via the projects SIRIUS, Euromed Justice and Euromed Police). These institutions have not reviewed and are not responsible for the content of this request.
You are responsible for complying with the relevant laws and procedure regarding data categorization and privacy when making and processing any request.

LEGAL BASIS:

DOMESTIC LEGAL PROCESS:

If required by the service provider, attach the domestic legal process for the requested data in accordance with legislation in your country.

Delete file

Attach file

CONCERNED USER(S) OR ACCOUNT(S):

Delete file

Attach file

☐ Indicate if you have previously submitted a preservation request for the account(s).

INFORMATION REQUESTED TO AVERT THE EMERGENCY:

This request applies to the items indicated below, whether in electronic or other form, including information stored on backup media, if available. A justification for the request for disclosure of these datasets will follow.address(es)

- ☐ Full name provided
- ☐ Vanity name, nickname or login name
- ☐ User ID
- ☐ Phone number(s)
- ☐ Email address(es)
- ☐ Date of birth
- ☐ Copy of ID card or passport provided by the subscriber
- ☐ Billing information/means of payment
- ☐ Account start and end date
- ☐ Account status
- ☐ Registration IP address, including time stamp
- ☐ Associated devices (including device ID, IMEI, MAC address and UDID when available)

- Type of registration, copy of a contract, means of verification of identity at the moment of registration, copies of documents provided by the subscriber
- Any other information pertaining to the identity of the user/subscription holder

For registries and registrars:

- Registrant, technical and administrative name, address, phone, fax number and email address of the specified domain
- Creation, updated date, current status and name servers of the specified domain

Other information:

Traffic data

- IP address logs, including time stamp
- Message logs and chat logs
- Activity log/logfiles, including time stamp
- Routing information (source IP address, destination IP address, port number, browser, email header, message ID, data transfer volume, source or destination of any electronic messages sent from or received from the account)
- Cryptocurrency address(es)

Other information:

Content data

- Contacts
- Messages
- Posts
- Media files: videos, photos, documents
- Profile photo(s)
- Mailbox dump
- Device backup
- Geolocation data, including time stamp
- Deposit/withdrawal/transaction history

Other information:

Other data

JUSTIFICATION, INCLUDING FOR NECESSITY AND PROPORTIONALITY:

TIME RANGE/PERIOD:

CONFIDENTIALITY:

☐ I request that you do not disclose the existence of this request to the subscriber or any other person, other than as necessary to comply with this request. If compliance with this request might result in a permanent or temporary termination of service to the account(s), or otherwise alert any user of the account(s) as to your actions to disclose the information described above, please contact me as soon as possible before taking action.

Attach court order if available

Attach file

PGP:

Attach PGP public key (if applicable)

Attach file

SUMMARY OF DOCUMENTS ATTACHED:

Open attachments pane

EMERGENCY DISCLOSURE REQUEST 4

If you have questions regarding this request, please contact me.

I hereby certify I have the legal authority to submit this request and that the information provided is true to the best of my knowledge.

Insert stamp

Delete stamp

Insert signature

Delete signature

SIGN ELECTRONICALLY (once electronically signed the request cannot be edited)

Insert digital signature

Insert signature and stamp as images, sign the document electronically or print, stamp and sign it using a blue or black pen.

Best practices

Save editable

Print

Finalize

EMERGENCY DISCLOSURE REQUEST **5**

ANNEX IV. MODEL DIRECT REQUEST FORM FOR VOLUNTARY DISCLOSURE

The forms, as included in this publication, are for reference and training purposes. In order to make edits to these forms, practitioners must download the forms' interactive version from the UNODC Sherloc Electronic Evidence Hub: https://sherloc.unodc.org/cld/en/st/evidence/model-forms.html.

INSERT LETTERHEAD OF THE REQUESTING AUTHORITY HERE

REQUEST FOR DISCLOSURE OF DATA ON A VOLUNTARY BASIS

Date

REQUESTING AUTHORITY:

Identification details

Full name or personal identification number

Position held

Contact details of authority's representative

Official email address and phone number

Proceedings number

Case number **Previous request numbers**

ADDRESSEE (RECIPIENT):

Address

This authority is conducting a criminal investigation that involves one or multiple users from your platform. Electronic data has been deemed relevant in this matter. I am hereby requesting the disclosure of electronic data on a voluntary basis in relation to the below mentioned user(s) and/or account(s).

Any and all information or data provided in response to this request will only be used in the described investigation and will not be disclosed to unauthorized personnel.

NATURE OF THE CASE:

Attach file

REQUEST FOR DISCLOSURE OF DATA ON A VOLUNTARY BASIS 1

This model form is provided by UNODC, UN CTED, Europol, Eurojust and Cepol (via the projects SIRIUS, Euromed Justice and Euromed Police). These institutions have not reviewed and are not responsible for the content of this request.
You are responsible for complying with the relevant laws and procedure regarding data categorization and privacy when making and processing any request.

LEGAL BASIS:

DOMESTIC LEGAL PROCESS:

If required by the service provider, attach the domestic legal process for the requested data in accordance with legislation in your country.

Delete file

Attach file

CONCERNED USER(S) OR ACCOUNT(S):

Delete file

Attach file

✓ Indicate if you have previously submitted a preservation request for the account(s).

INFORMATION REQUESTED:

This request applies to the items indicated below, whether in electronic or other form, including information stored on backup media, if available. A justification for the request for disclosure of these datasets will follow.

- ☐ Full name provided
- ☐ Vanity name, nickname or login name
- ☐ User ID
- ☐ Phone number(s)
- ☐ Email address(es)
- ☐ Date of birth
- ☐ Billing information/means of payment
- ☐ Account start and end date
- ☐ Account status
- ☐ Registration IP address, including time stamp
- ☐ Associated devices (including device ID, IMEI, MAC address and UDID when available)
- ☐ Copy of ID card or passport provided by the subscriber
- ☐ Type of registration, copy of a contract, means of verification of identity at the moment of registration, copies of documents provided by the subscriber
- ☐ Any other information pertaining to the identity of the user/subscription holder

REQUEST FOR DISCLOSURE OF DATA ON A VOLUNTARY BASIS 2

For registries and registrars:

- Registrant, technical and administrative name, address, phone, fax number and email address of the specified domain
- Creation, updated date, current status and name servers of the specified domain

Other information:

Traffic data

- IP address logs, including time stamp
- Message logs and chat logs
- Activity log/logfiles, including time stamp
- Routing information (source IP address, destination IP address, port number, browser, email header, message ID, data transfer volume, source or destination of any electronic messages sent from or received from the account)
- Cryptocurrency address(es)

Other information:

Other data

JUSTIFICATION, INCLUDING FOR NECESSITY AND PROPORTIONALITY:

TIME RANGE/PERIOD:

CONFIDENTIALITY:

☐ I request that you do not disclose the existence of this request to the subscriber or any other person, other than as necessary to comply with this request. If compliance with this request might result in a permanent or temporary termination of service to the account(s), or otherwise alert any user of the account(s) as to your actions to disclose the information described above, please contact me as soon as possible before taking action.

Attach court order if available

Attach file

PGP:

Attach PGP public key (if applicable)

Attach file

SUMMARY OF DOCUMENTS ATTACHED:

Open attachments pane

If you have questions regarding this request, please contact me.

I hereby certify I have the legal authority to submit this request and that the information provided is true to the best of my knowledge.

Insert stamp

Delete stamp

Insert signature

Delete signature

SIGN ELECTRONICALLY (once electronically signed the request cannot be edited)

Insert digital signature

- **Insert signature and stamp as images, then sign the document electronically;**
- **<u>OR</u> print to sign and stamp the document manually, please use a black or blue pen.**

Best practices

Save editable

Print to sign and stamp manually

Finalize

ANNEX V. DATA RETENTION LAWS FOR SELECTED STATES

AUSTRALIA

In 2017, new Australian laws requiring the retention of certain data came into effect. Under section 187AA of the Telecommunications (Interception and Access) Act 1997 (Cth), telecommunications companies (which include SPs) must store particular customer data for at least two years, including BSI and traffic data, but not content.

BRAZIL

The Civil Rights Framework on Internet – Law n. 12.965/2014 provides for data retention as follows:

- Article 13: Internet connection records must be retained for 1 year.
- Article 15: Internet applications access logs must be retained for 6 months.

Both data can be subject of a preservation request and of an extension of preservation.

CANADA

The Personal Information Protection and Electronic Documents Act (PIPEDA)) is the federal privacy law for private-sector organizations. It sets out the ground rules for how businesses must handle personal information in the course of commercial activity. Privacy laws considered substantially similar to PIPEDA have also been enacted in many provinces in Canada (British Columbia, Alberta, Ontario, Quebec, New Brunswick, Nova Scotia and Newfoundland).

ITALY

A mandatory data retention period is established only for traffic data regarding Internet service providers and telecommunication service providers, while other operators are free to choose their own policy on data retention of computer data.

For the first ones, the legal regime may differ depending on the seriousness of the crime investigated. In this regard, the standard regime is ruled by Art. 132 Legislative Decree no. 196/2003 (Personal Data Protection Code), according to which the retention period is as follows:

- Telephone traffic data: 24 months
- Unsuccessful/missed calls traffic data: 30 days
- Electronic communication traffic data: 12 months

NORWAY

Data held by SPs must be deleted within 21 days.

RUSSIAN FEDERATION

The 2016 anti-terrorist federal law 374-FZ known as Yarovaya Law and the Resolution of the Government of the Russian Federation of 16.12.2017 № 1576 "On amending of the Resolution of the Government of the Russian Federation of 31.07.2014 г. № 759" require all telecommunication providers (including Internet providers) to store content data for six months (as of 17 January 2018), and traffic data and BSI for one and three years, respectively.

SERBIA

On 29 June 2010, the Serbian parliament adopted the Law on Electronic Communications, requiring SPs to retain electronic communications for 12 months.

SWITZERLAND

As of 7 July 2016, the Swiss Federal Law on Surveillance of the Post and Telecommunications entered into force. All SPs must retain designated sets of data for six months.

THAILAND

Section 26 of the Computer Crime Act B.E. 2550 (2007) provides that an SP must retain computer traffic data for at least 90 days from the date on which the data is put into a computer system, however, if necessary, a relevant competent official may instruct an SP to retain such data for a period of longer than 90 days but not exceeding two years on a special case-by-case basis or on a temporary basis.

UNITED STATES OF AMERICA

No mandatory data retention laws.

GLOSSARY

Central authority
The authority that has the responsibility and powers to send and receive requests for mutual legal assistance and either to execute them or to transmit them to the competent authorities for execution.

Mutual legal assistance (MLA)
The provision of assistance, usually in the gathering and transmission of evidence by a competent authority of one State to that of another, in response to a written request for assistance.

Mutual legal assistance request
Term used for the formal written document by which mutual legal assistance can be made (in French, a commission rogatoire), also known as a letter of request.

Police-to-police cooperation
This includes law enforcement officers from a one State directly contacting counterparts for assistance in another.

Requested State
Refers to a State executing a mutual legal assistance request from a requesting State.

Requesting State
Refers to a State requesting mutual legal assistance in the gathering and transmission of evidence by a competent authority of one State.

State authorities
State authorities in this document refers to competent authorities for requesting e-evidence in the cross-border context, and they may include law enforcement, prosecution, judiciary and/or central authority depending on the jurisdiction.

V.21-03092